

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MONTANA  
BUTTE DIVISION**

IN RE: SNOWFLAKE, INC. DATA  
SECURITY BREACH LITIGATION

**Case No. 2:24-md-03126-BMM**

---

**FINANCIAL INSTITUTION PLAINTIFF'S**  
**REPRESENTATIVE CLASS ACTION COMPLAINT**

## **TABLE OF CONTENTS**

<b>INTRODUCTION .....</b>	<b>1</b>
<b>PARTIES .....</b>	<b>6</b>
I.    Plaintiff .....	6
II.   Defendants .....	7
<b>JURISDICTION AND VENUE .....</b>	<b>8</b>
<b>FACTUAL ALLEGATIONS .....</b>	<b>10</b>
<b>PART ONE: THE DATA BREACH.....</b>	<b>10</b>
I.    Ticketmaster Uses Snowflake Data Cloud Platform to Store PCD.....	12
II.   Multiple, basic cybersecurity failures led to the Data Breach .....	14
III.  Relevant industry standards and regulations for data security were not followed by Snowflake or Ticketmaster .....	21
A.   The Federal Trade Commission’s straightforward guidelines were not followed .....	21
B.   Payment Card Industry Data Security Standards were not followed.....	26
C.   Other standards applicable to cloud storage were not followed.....	30
IV.   The Data Breach harmed Plaintiff and Class Members.....	32
A.   The Data Breach caused immediate damages to Plaintiff and Class Members .....	33

<b>PART TWO: TICKETMASTER AND LIVE NATION</b>	34
I. Ticketmaster’s business and data security promises	34
II. Ticketmaster owed a duty of care to Plaintiff and Class Members	41
III. Ticketmaster breached its duty to protect PCD and personal information	43
IV. The PCD and personal information of Plaintiff’s and Class Members’ customers was stolen	52
<b>PART THREE: SNOWFLAKE</b>	54
I. Snowflake had a duty to safeguard Plaintiff’s and Class Members’ information	58
II. Snowflake delayed notification and denied responsibility for its negligent security failures	59
III. Snowflake’s negligence as a sophisticated cloud-storage services provider	61
IV. Snowflake breached its duty and engaged in unfair trade practices	63
<b>PART FOUR: PLAINTIFF’S INJURIES</b>	67
<b>CLASS ACTION ALLEGATIONS</b>	68
<b>CAUSES OF ACTION</b>	73
<b>PRAYER FOR RELIEF</b>	84
<b>DEMAND FOR JURY TRIAL</b>	86

## **INTRODUCTION**

1. Data companies are acutely aware of the critical importance of cybersecurity in an increasingly interconnected world. With the exponential growth of cloud storage, companies are entrusted with highly sensitive and protected information, ranging from personal details to financial records.

2. This is a “hub-and-spoke” data breach case. The “hub” in this case is Defendant Snowflake, Inc. (“Snowflake”), which is a company that specializes in cloud-storage technologies to warehouse and secure sensitive data, and in selling data storage and analytics products. Snowflake sells its data storage services to numerous companies, or “spokes,” who store information on Snowflake’s data cloud, including Defendants Ticketmaster, LLC and Live Nation Entertainment, Inc. (collectively “Ticketmaster”). Ticketmaster is just one of the thousands of companies<sup>1</sup> that utilize Snowflake’s data storage and products, many of which are also Fortune 500 or publicly traded companies including AT&T, Advance Auto Parts, Pfizer, and LendingTree.

---

<sup>1</sup> Snowflake Fast Facts Sheet, accessible at: <https://www.clearintelligence.com/wp-content/uploads/2024/09/SnowflakeFastFactsSheet.pdf> (last visited Mar. 20, 2025); Snowflake, *How It All Started*, <https://www.snowflake.com/en/company/overview/about-snowflake/> (last visited Mar. 20, 2025).

3. Stressing to investors that it built its data-storage product “with security as a core tenet,”<sup>2</sup> Snowflake has long understood and acknowledged the importance of robust cybersecurity to protect its customers’ highly sensitive data.

4. Similarly, Ticketmaster has also long understood the importance of robust cybersecurity to protect their own customers’ data, from which Ticketmaster extracts a handsome profit.

5. Information security policies, procedures, and practices are imperative to ensure that private, sensitive information is not exposed to unauthorized third parties. These exposures, commonly referred to as “data breaches” or “security incidents” can cause significant harm to both individuals and financial institutions.

6. Plaintiff New Orleans Firemen’s Federal Credit Union (“Plaintiff” or “NOFFCU”) and the Class Members are financial institutions that issue payment cards, such as debit or credit cards, to their customers. Payment Card Data (“PCD”) is highly sensitive and private information which includes cardholder name, credit or debit card number, expiration date, cardholder verification value, and service code.

7. Ticketmaster accepts customer payment cards for the purchase of goods and services. The payment card information is entered onto Ticketmaster’s

---

<sup>2</sup> Snowflake Inc. 2024 Annual Report (Form 10-K) at 15 (Mar. 26, 2024) (“Snowflake 2024 10-K”), <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001640147/264ea0e0-8e73-4f07-9f54-78ab341a2c79.pdf> (last visited Mar. 20, 2025).

website, app or the payment card is inserted, tapped, or swiped on a point of sale (“POS”) terminal at a venue to complete the transaction.

8. Ticketmaster operates a digital ticketing platform that requires customers to provide their PCD to purchase its products, including event tickets. To purchase products from Ticketmaster, customers are required to entrust Ticketmaster with their PCD. This information is ultimately stored in Ticketmaster’s Snowflake account. In return, Plaintiff and the Class reasonably expect that Snowflake and Ticketmaster (collectively “Defendants”) will safeguard that PCD. A single data breach can result in significant repercussions for financial institutions. As a result, and based upon legal and industry-standard requirements, companies prioritize robust cybersecurity measures.

9. Here, however, neither Snowflake nor Ticketmaster implemented three of the most basic and industry-standard cybersecurity policies and practices to protect PCD and other sensitive personal information, including, most prominently, multifactor authentication (MFA).<sup>3</sup>

10. The foreseeable result of Defendants’ failures: a massive data breach (“Data Breach”), wherein the cybercriminal group known by codename UNC5537

---

<sup>3</sup> “PCD” as used herein, refers to that information which was exposed to cybercriminals through the Data Breach. Both Ticketmaster and Snowflake protected this private data behind credentials (i.e., a username and password), intending that it would not be exposed to unauthorized third parties. As alleged herein, inadequate, negligent, and reckless cybersecurity practices resulted in that information being exposed.

took compromised login credentials for Defendants, which they then used to access Ticketmaster's Snowflake accounts, and successfully exfiltrated sensitive PCD and other personal information belonging to millions of consumers.

11. UNC5537's success was enabled by Snowflake's and Ticketmaster's basic data security failings. Defendants collectively ignored relevant governmental guidance, regulations, statutes, industry standards, and best practices.

12. The Data Breach's foreseeable consequences are neither imaginary nor hypothetical: shortly after the Data Breach, consumers' sensitive personal information and PCD, previously stored with Snowflake, began appearing for sale on the dark web.<sup>4</sup>

13. On or about December 17, 2024, Visa, a payment card services corporation, issued a series of alerts to financial institutions, including Plaintiff, notifying them of a potential network intrusion at Ticketmaster which placed payment account information at risk. Visa further indicated that PCD, specifically payment account numbers, had been potentially compromised. Visa further estimated that the "exposure window" for Ticketmaster included PCD from May 18, 2009 through May 18, 2019.

---

<sup>4</sup> Snowflake Breach Threat Actor Offers Data of Cloud Company's Customers, SOCRadar, <https://socradar.io/overview-of-the-snowflake-breach/> (last visited Mar. 20, 2025).

14. As a direct and proximate result of Defendants' failure to implement and follow basic security procedures, Plaintiff and Class Members have been injured by the Data Breach. Not only have cybercriminals obtained Plaintiff's customers' valuable and sensitive PCD and personal information about them, but that information has been obtained by other criminals and offered for resale to still more criminals.

15. Plaintiff and Class Members have already suffered significant financial damages: resources spent notifying their customers that their payment cards were exposed to unauthorized third parties in the Data Breach, canceling and reissuing payment cards to mitigate the imminent and substantial risk of PCD misuse, covering fraudulent charges, as well as other damages.

16. Plaintiff brings this class action to remedy the financial losses and other harms it has suffered and continues to suffer, as well as the impending risk of future harm that is likely to occur in the form of future fraudulent banking activity as a direct result of Defendants' failure to secure Plaintiff's and the Class's PCD.

17. Plaintiff, individually and on behalf of a class of financial institutions, seeks monetary and non-monetary relief and asserts claims against Defendants for negligence (including negligence *per se*), unjust enrichment, and declaratory judgment.



18. Each Defendant bears responsibility for its role in the Data Breach. Despite their experience and sophistication, Defendants were negligent and reckless in failing to implement reasonable, basic, and routinely required cybersecurity policies and practices to protect Plaintiff's and Class Members' PCD.

## **PARTIES**

### **I. Plaintiff**

19. **New Orleans Firemen's Federal Credit Union** ("NOFFCU") is a federally chartered credit union with its principal place of business in Metairie, Louisiana. NOFFCU is the second oldest federally chartered credit union in the nation, serving over 28,000 members and more than 400 business partners across Louisiana and Mississippi. As a result of the Data Breach, NOFFCU has suffered, and continues to suffer, injury, including, among other things, costs to cancel and reissue payment cards compromised in the Data Breach, costs to refund fraudulent charges, costs due to the time and expense associated with investigating the Data Breach and communicating with its customers about cards that were exposed in the Data Breach, costs of fraud monitoring, and costs due to lost interest and transaction fees due to reduced payment card usage.

## II. Defendants

20. **Snowflake Inc.** is a cloud-based data storage company incorporated under Delaware law, with its principal place of business located at 106 E. Babcock Street, Suite 3A, Bozeman, Montana.<sup>5</sup>

21. **Ticketmaster, LLC** is a ticket distribution company for entertainment events and is a wholly owned subsidiary of Live Nation.<sup>6</sup> Ticketmaster is a Virginia limited liability company, with its principal place of business located at 9348 Civic Center Drive, Beverly Hills, California.<sup>7</sup>

22. **Live Nation Entertainment, Inc.** (“Live Nation”) is an entertainment company incorporated under Delaware law, with its principal place of business located at 9348 Civic Center Drive, Beverly Hills, California.<sup>8</sup>

23. Throughout the events at issue, Defendants Live Nation and Ticketmaster, LLC have operated as one entity. Live Nation purchased Ticketmaster, LLC in 2009. Live Nation has used Ticketmaster, LLC as a dependent and integrated division rather than as a separate legal entity. Live Nation describes Ticketmaster, LLC as one of the company’s three “divisions” along with

---

<sup>5</sup> Snowflake Inc. 2024 10-K at 1.

<sup>6</sup> Live Nation 2023 10-K at 54.

<sup>7</sup> Ticketmaster, LLC, *Statement of Information*, Cal. Sec’y of State (Mar. 20, 2025), <https://bizfileonline.sos.ca.gov/api/report/GetImageByNum/253133124121113249074045085047228112143236158047> (last visited Mar. 20, 2025).

<sup>8</sup> Live Nation Entertainment, Inc., Annual Report (Form 10-K) (Feb. 22, 2024) (“Live Nation 2023 10-K”), <https://www.sec.gov/Archives/edgar/data/1335258/000133525824000017/lyv-20231231.htm>. (last visited Mar. 20, 2025).

Concerts and Sponsorship. The business operations are fully coordinated and shared. Resources are cross-applied without recognizing full and complete cost and profit centers. Live Nation and Ticketmaster, LLC share a corporate headquarters. Ticketmaster LLC's top executives, including its President, COO and Chief Technology Officer are listed as executives of Live Nation. Management decisions at Ticketmaster, LLC are made by and through the management of Live Nation. The management of Live Nation and Ticketmaster, LLC were and are directly involved in the events at issue in this litigation, including cybersecurity, the Data Breach itself, and Defendants' response to the Data Breach.

24. Whenever reference in this Complaint is made to any act or transaction of Ticketmaster, LLC and Live Nation Entertainment, Inc. (collectively "Ticketmaster"), such allocations shall be deemed to mean that the principals, officers, employees, agents, and/or representatives of Ticketmaster committed, knew of, performed, authorized, ratified and/or directed such transaction on behalf of Defendants Ticketmaster, LLC and Live Nation Entertainment, Inc. while actively engaged in the scope of their duties.

### **JURISDICTION AND VENUE**

25. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d). The aggregated claims of the individual Class Members exceed the sum or value of \$5,000,000 exclusive of

interest and costs; there are more than 100 putative class members; and minimal diversity exists because at least one member of the putative class is a citizen of a different state than Defendants.

26. This Court has personal jurisdiction over Snowflake because its headquarters and principal place of business is in Bozeman, Montana.

27. This Court has personal jurisdiction over Ticketmaster because Ticketmaster is registered to conduct business in Montana, Ticketmaster has conducted business in Montana, including through its acquisition of a majority stake in Logjam Presents, the leading promoter and operator venue in Montana, Ticketmaster regularly conducts business in Montana. Ticketmaster's sale of tickets in Montana has resulted in the storage of Montana residents' PCD on Snowflake servers, which was then stolen in the Data Breach. Ticketmaster has sufficient minimum contacts in Montana and intentionally avails itself of this jurisdiction by conducting its corporate operations here and promoting, selling, and marketing products and services to Montana financial institutions, consumers, and other entities.

28. Venue is proper in this District under 28 U.S.C. §1391(a) because Defendant Snowflake's principal place of business is in Montana, and a substantial part of the events, acts, and omissions giving rise to the claims of Plaintiff and the Class occurred in this District.

## **FACTUAL ALLEGATIONS**

### **PART ONE: THE DATA BREACH**

29. Snowflake is one of the largest data storage providers in the United States and it contracts with thousands of organizations around the world to securely store their consumer and employee data on its “Data Cloud” platform.<sup>9</sup> Snowflake’s platform is a product and a service that provides companies the ability to store, process, and analyze large volumes of consumer and employee data.<sup>10</sup>

30. Snowflake’s product is typically referred to as “Software as a Service” (SaaS), which refers to the fact that Snowflake’s software allows its customers to connect to cloud-based applications over the internet.

31. During the regular course of providing its Data Cloud platform to its customers, Snowflake is provided and entrusted with certain information, including PCD. As Snowflake itself has stated, “Snowflake manages all aspects of how this data is stored—the organization, file size, structure, compression, metadata, statistics, and other aspects of data storage are handled by Snowflake.”<sup>11</sup>

32. As a major provider of cloud computing services, Snowflake advertises that it “sets the standard for data security” and further represents that its

---

<sup>9</sup> Snowflake, *How It All Started*, <https://www.snowflake.com/en/company/overview/about-snowflake/> (last visited Mar. 20, 2025).

<sup>10</sup> Snowflake, *The Snowflake Platform*, <https://www.snowflake.com/en/data-cloud/platform/> (last visited Mar. 20, 2025).

<sup>11</sup> *Key Concepts & Architecture*, SNOWFLAKE, <https://docs.snowflake.com/en/user-guide/intro-key-concepts> (last visited Mar. 20, 2025).

cloud computing platform “follows world-class, standards-based practices for the controls and processes that secure it and is based on a multilayered security architecture to protect customer data and access to that data.” Snowflake also states that its “security architecture is completed by the monitoring, alerts, controls, and processes that are part of Snowflake’s comprehensive security framework.”<sup>12</sup>

33. Snowflake also recognizes the importance of maintaining adequate data security for its cloud computing platform users: “In today’s connected world where cybercriminals have greater opportunity than ever before, data security is crucial for every business.” Snowflake also recommends data security solutions that companies can implement; a list that includes Identity and Access Management (“IAM”) strategies.<sup>13</sup>

34. IAM systems apply individualized access controls through, inter alia, authentication such as MFA.<sup>14</sup> MFA is an electronic authentication method “that requires more than one distinct authentication factor” for a user to be granted access to a website or application.<sup>15</sup> Examples of MFA include the combination of both an account password and a single-use password sent via text message to a user’s mobile phone to access an account.

---

<sup>12</sup> *Intro to Data Security*, SNOWFLAKE, <https://www.snowflake.com/trending/intro-to-data-security/> (last visited Mar. 20, 2025).

<sup>13</sup> *Id.*

<sup>14</sup> Matthew Kosinski and Amber Forrest, *What is IAM?*, IBM (Jan. 22, 2024), <https://www.ibm.com/topics/identity-access-management>. (last visited Mar. 20, 2025).

<sup>15</sup> *Id.*

35. MFA has become an “increasingly important” piece of IAM strategies as standard one-factor authentication, which relies on only usernames and passwords, is not difficult to break. Indeed, compromised login credentials are a leading cause of data breaches, and MFA adds an extra layer of protection. So “[e]ven if hackers steal a password, it won’t be enough to gain unauthorized access to a system.”<sup>16</sup>

36. Even though Snowflake supports MFA to provide increased security for its customers accessing the Snowflake platform and recommends that its customers implement MFA, Snowflake did not require its customers, including Ticketmaster, to use MFA or automatically enroll its customers, including Ticketmaster, into MFA prior to the Data Breach.<sup>17</sup> Nor did Ticketmaster enroll in Snowflake’s MFA to access its Snowflake account.

#### **I. Ticketmaster Uses Snowflake Data Cloud Platform to Store PCD**

37. Ticketmaster is a Snowflake customer and stores its customers’ PCD and personal information on the Data Cloud.

38. Ticketmaster accepts customer payment cards for the purchase of goods and services. The payment card information is entered into Ticketmaster’s

---

<sup>16</sup> *Id.*

<sup>17</sup> *Multi-factor authentication (MFA)*, SNOWFLAKE, <https://docs.snowflake.com/user-guide/security-mfa> (last visited Mar. 20, 2025).

website, app, or the payment card is inserted, tapped, or swiped on a point of sale (“POS”) terminal at a venue to complete the transaction on behalf of a customer.

39. PCD is highly valuable and often targeted by hackers because it can be used to make fraudulent transactions. Well-publicized data breaches involving PCD have occurred at multiple companies in the recent past, putting Defendants on notice that Snowflake’s cloud storage platforms would be targeted by cyber criminals.

40. Despite widespread publicity about other data breaches and industry alerts regarding these other notable data breaches, Defendants failed to take reasonable steps to adequately protect their computer or data systems from being breached.

41. Ticketmaster’s sales are made to customers using PCD. Ticketmaster customers purchase concert tickets by entering their PCD into the Ticketmaster website, or app or by tapping/swiping at the point-of-sale. After the credit/debit card is inserted, tapped or swiped or the credit/debit card data is entered into Ticketmaster’s website or app, Ticketmaster uses one of several payment processing networks (*e.g.*, Visa or MasterCard) to transmit a request for authorization to the financial institution that issued the payment card (*e.g.*, Plaintiff). The issuing institution authorizes the payment, and Ticketmaster electronically forwards a receipt of the transaction to another financial institution,



known as the “acquiring bank,” which contracts with the merchant to process credit and debit card transactions on the merchant’s behalf. The acquiring bank then forwards the funds to the merchant to satisfy the transaction and is reimbursed by the issuing financial institution (*e.g.*, Plaintiff). At which point, the issuing institution posts the debit or credit transaction to its customer’s account.

42. Defendants knew that if they failed to properly secure or safeguard their customers’ PCD, there was a high likelihood that hackers would breach Defendants’ systems and steal the PCD of Defendants’ customers, which would cause significant costs to issuing financial institutions, such as Plaintiff and Class Members.

## **II. Multiple, basic cybersecurity failures led to the Data Breach.<sup>18</sup>**

43. The events leading up to and following the Data Breach are summarized in a June 10, 2024, report published by Mandiant (the “Mandiant Report”), a cybersecurity firm that assisted Snowflake in its investigation of the Data Breach.<sup>19</sup>

---

<sup>18</sup> Additional details regarding the breach will be revealed through discovery, including information related to a report prepared by another, reputable cybersecurity company, which was demanded to be taken off the internet by Snowflake. *See* Part Two, *infra*.

<sup>19</sup> Mandiant, *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, Google Cloud (June 10, 2024), <https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion> (cited to hereinafter as “*Mandiant Report*”) (last visited Mar. 20, 2025). Since Snowflake had a hand in the *Mandiant Report*, the events are likely worse than presented, and will be clarified in discovery. *See also* *Snowflake Breach: Hacker Confirms Access Through Infostealer Infection*, Hudson Rock, <https://archive.is/tljkW> (“Hudson Rock Report,” archived website) (last visited Mar. 20, 2025).

44. Beginning on or around April 2024, a cybercriminal group named UNC5537 carried out a successful cyberattack on Snowflake, exfiltrating the data of hundreds of Snowflake customers, including Ticketmaster.

45. UNC5537 is a known cybercriminal group likely comprised of hackers in North America. A financially motivated threat actor, UNC5537 employs information-stealing malware to infiltrate systems, collect user data, exfiltrate that data, and then sell it on underground cybercrime forums or sell the information to other hackers.<sup>20</sup>

46. UNC5537's successful cyberattack on Snowflake and Ticketmaster was simple and could have easily been prevented. As the Mandiant Report put it, the cyberattack was “not the result of any particularly novel or sophisticated tool, technique, or procedure” but was the consequence of “missed opportunities” on the part of Snowflake and Ticketmaster to properly secure their credentials.<sup>21</sup>

47. UNC5537's cyberattack transpired in two basic steps. First, UNC5537 gained access to a customer's Snowflake credentials—i.e., their username and password. Stolen credentials are common and represent a well-known and easily

---

<sup>20</sup> UNC5537 Summary, Mphasis (June 17, 2024), <https://www.mphasis.com/content/dam/mphasis-com/global/en/home/services/cybersecurity/june-17-19-unc5537.pdf>. (last visited Mar. 20, 2025).

<sup>21</sup> *Mandiant Report*, *supra* n. 19.

anticipated risk by cybersecurity companies.<sup>22</sup> According to the Mandiant Report, UNC5537 was also “likely able to aggregate credentials” for a large number of Snowflake customers, such as Ticketmaster, by simply perusing various sources of previously stolen credentials, as “large lists of stolen credentials exist both for free and for purchase inside and outside of the dark web.”<sup>23</sup>

48. Next, UNC5537 simply used the stolen credentials to log into a Snowflake customer’s account and exfiltrate customer data.<sup>24</sup>

49. According to the Mandiant Report, the success of UNC5537’s straightforward cyberattack was made possible by “three primary factors” on the part of Snowflake and Ticketmaster.<sup>25</sup>

50. First, Ticketmaster did not have MFA enabled, nor did Snowflake require them to have MFA enabled. MFA is a basic and industry-standard cybersecurity measure, available for nearly three decades,<sup>26</sup> that requires a user to,

---

<sup>22</sup> See TJ Alldridge, *Stolen Credentials Make You Question Who Really Has Access*, Mandiant (Feb. 13, 2024), <https://cloud.google.com/blog/products/identity-security/stolen-credentials-make-you-question-who-really-has-access> (“stolen credentials are the third most used infection vector behind exploits and phishing”) (last visited Mar. 20, 2025).

<sup>23</sup> *Mandiant Report*, *supra* n. 19 **Error! Bookmark not defined.**

<sup>24</sup> *Id.*

<sup>25</sup> See also Brad Jones, *Detecting and Preventing Unauthorized User Access*, Snowflake (June 2, 2024), *Detecting and Preventing Unauthorized User Access - Cybersecurity - Snowflake* (Snowflake recommending MFA, trusted locations, and resetting credentials) (last visited Mar. 20, 2025).

<sup>26</sup> Bojan Šimić, *Identity in the Digital Age and the Rise of Multi-Factor Verification*, Forbes (Oct. 10, 2024), <https://www.forbes.com/councils/forbestechcouncil/2024/10/10/identity-in-the-digital-age-and-the-rise-of-multi-factor-verification/> (MFA was developed by AT&T as a system to exchange codes on two-way pagers) (last visited Mar. 20, 2025).

in addition to providing their username and password, further authenticate their identity through another source, such as through a passcode sent by text message or email.<sup>27</sup> Without MFA, a valid username and password were all UNC5537 needed to access Ticketmaster’s customer data.

51. Strikingly, even though the federal government has urged companies to use MFA to secure data since 2016,<sup>28</sup> and Snowflake offered “free and available” MFA to customers since June 2015,<sup>29</sup> at the time of the Data Breach, Snowflake’s default setting had MFA turned off. Moreover, Snowflake customers, including Ticketmaster, did not have the ability to require their users to use MFA.

52. Snowflake changed policies shortly after the Data Breach. On July 9, 2024, Snowflake announced that customers, like Ticketmaster, could now enforce MFA for its users and monitor MFA compliance.<sup>30</sup> And on September 13, 2024, Snowflake announced a new policy which, for the first time, established a default

---

<sup>27</sup> Rose de Fremery, *Tracing the Evolution of Multi-Factor Authentication*, LastPass (Oct. 16, 2023), <https://blog.lastpass.com/posts/tracing-the-evolution-of-multi-factor-authentication> (last visited Mar. 20, 2025).

<sup>28</sup> *Fact Sheet: Cybersecurity National Action Plan*, The White House (Feb. 9, 2016), <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>. (last visited Mar. 20, 2025).

<sup>29</sup> Snowflake Advances Cybersecurity Excellence by Joining CISA Secure by Design Pledge (July 29, 2024), <https://www.snowflake.com/en/blog/snowflake-cybersecurity-cisa-secure-by-design/>. Snowflake has also used MFA to protect its own systems. Mihir Bagwe, *The Snowballing of the Snowflake Breach: All About the Massive Snowflake Data Breach*, CyberExpress (June 17, 2024), <https://thecyberexpress.com/all-about-massive-snowflake-breach/>. (last visited Mar. 20, 2025).

<sup>30</sup> Brad Jones & Anoosh Saboori, *Snowflake Admins Can Now Enforce Mandatory MFA*, Snowflake (July 9, 2024), <https://www.snowflake.com/en/blog/snowflake-admins-enforce-mandatory-mfa/>. (last visited Mar. 20, 2025).

setting *requiring* MFA for users of Snowflake accounts created as of October 2024.<sup>31</sup>

53. Second, Defendants did not have policies and procedures in place to rotate or disable stale credentials. Notably, many of the credentials stolen by UNC5537 through malware were old and were originally stolen through various malware attacks dating as far back as 2020. But without policies or procedures in place to rotate or disable such stale credentials, the years-old credentials remained valid and allowed UNC5537 to exfiltrate Snowflake customers' data.

54. Addressing the issue of stolen credentials, Snowflake now advertises that it automatically disables leaked passwords detected on the dark web.<sup>32</sup> This technology is and was also available to Ticketmaster.

55. Third, affected customers including Ticketmaster—did not restrict access to Snowflake cloud-based storage based upon certain trusted locations. Conditional Access Policies allow companies to fine-tune access to control from which devices and locations users can access resources. Again, without such

---

<sup>31</sup> Anoosh Saboori & Brad Jones, *Snowflake Strengthens Security with Default Multi-Factor Authentication and Stronger Password Policies*, Snowflake (Sept. 13, 2024), <https://www.snowflake.com/en/blog/multi-factor-identification-default/>. (last visited Mar. 20, 2025).

<sup>32</sup> Snowflake Will Automatically Disable Leaked Passwords Detected on the Dark Web, Snowflake (Nov. 14, 2024), <https://www.snowflake.com/en/blog/leaked-password-protection/>. (last visited Mar. 20, 2025).

protection, a valid username and password were all UNC5537 needed to access Ticketmaster's data from Snowflake anywhere at any time.

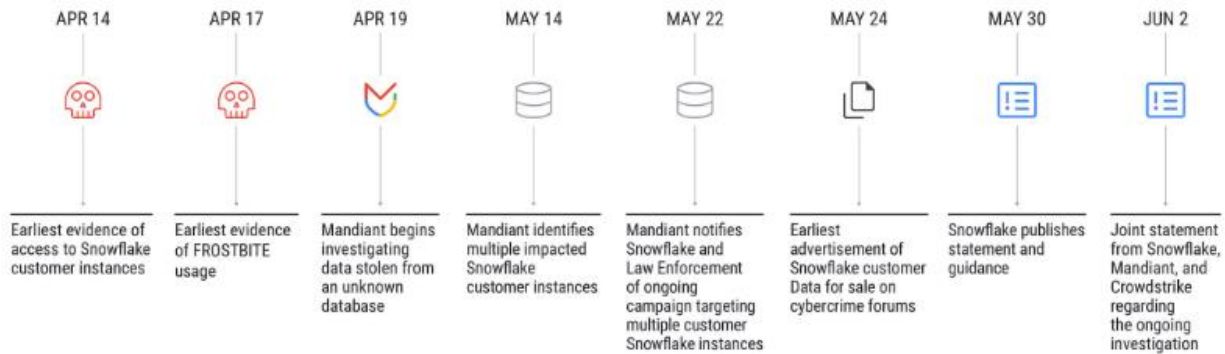
56. On May 30, 2024, Snowflake publicly disclosed the Data Breach for the first time through a blog post authored by CISO Brad Jones, which explained that Snowflake “became aware of potentially unauthorized access to certain customer accounts on May 23, 2024” and was “investigating an increase in cyber threat activity targeting some of our customers’ accounts.”<sup>33</sup>

57. The Mandiant Report documented the timeline of the Data Breach, which shows a concerning lag in Snowflake's response. As shown in the Mandiant Report timeline below, Snowflake did not make a public statement regarding the Data Breach until May 30, 2024. Snowflake's public disclosure occurred over a month and a half after Mandiant identified evidence of improper access to Snowflake customer data on April 14—but only a week after advertisements for the sale of stolen Snowflake customer data started showing up on cybercrime forums on May 24.<sup>34</sup>

---

<sup>33</sup> Brad Jones, *Detecting and Preventing Unauthorized User Access*, Snowflake (May 30, 2024), <https://snowflake.discourse.group/t/detecting-and-preventing-unauthorized-user-access/8967>. (last visited Mar. 20, 2025).

<sup>34</sup> *Mandiant Report*, *supra* n. 19.

UNC5537 Campaign Timeline

58. The Mandiant Report further found that UNC5537 was operating “with the intent of data theft and extortion” and was “advertising victim data for sale on cybercrime forums and attempting to extort many of the [customer] victims.”<sup>35</sup>

59. Plaintiff’s and Class Members’ PCD has already been sold and exchanged on the dark web between UNC5537 and various other cybercriminal threat actors such as Scattered Spider.<sup>36</sup>

60. The Mandiant Report concluded that UNC5537’s cyberattack “underscores the urgent need for credential monitoring, the universal enforcement of MFA and secure authentication, limiting traffic to trusted locations for crown jewels, and alerting on abnormal access attempts.”<sup>37</sup> Credential monitoring, MFA,

<sup>35</sup> *Id.*

<sup>36</sup> SC Staff, *Ransom demands issued to Snowflake hack victims*, SC Media (June 18, 2024), <https://www.scworld.com/brief/ransom-demands-issued-to-snowflake-hack-victims>. (last visited Mar. 21, 2025).

<sup>37</sup> *Mandiant Report*, *supra* n. 19.

limiting access, and alerts are all ubiquitous cybersecurity practices that have been standard for years.

**III. Relevant industry standards and regulations for data security were not followed by Snowflake or Ticketmaster.<sup>38</sup>**

**A. The Federal Trade Commission’s straightforward guidelines were not followed.**

61. The Federal Trade Commission (“FTC”) has issued guidance and taken enforcement actions that together illustrate the data security industry standards applicable to Snowflake and Ticketmaster.

62. Indeed, the FTC’s enforcement actions have established that a company’s failure to maintain reasonable and appropriate data security of consumer personal information violates the FTC Act’s prohibition on “unfair or deceptive acts.”<sup>39</sup>

---

<sup>38</sup> The below recitation of information security standards only provides an introduction as to applicable guidance. *See, e.g.*, NIST Update: Multi-Factor Authentication and SP 800-63 Digital Identity Guidelines, Federal Cybersecurity and Privacy Forum (Feb. 15, 2022), [https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal\\_Cybersecurity\\_and\\_Privacy\\_Forum\\_15Feb2022\\_NIST\\_Update\\_Multi-Factor\\_Authentication\\_and\\_SP800-63\\_Digital\\_Identity\\_%20Guidelines.pdf](https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_%20Guidelines.pdf). (last visited Mar. 21, 2025).

<sup>39</sup> *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 244-47 (3d Cir. 2015); Isabella Wright and Maia Hamin, “Reasonable” Cybersecurity in Forty-Seven Cases: *The Federal Trade Commission’s Enforcement Actions Against Unfair and Deceptive Cyber Practices*, DFR Lab (June 12, 2024), <https://dfrlab.org/2024/06/12/forty-seven-cases-ftc-cyber/>. (last visited Mar. 21, 2025).



63. In 2016, the FTC published guidance titled, *Protecting Personal Information: A Guide for Business* (the “FTC 2016 Guidance”).<sup>40</sup> The FTC 2016

Guidance:

- Stresses the importance of “[c]ontrol[ing] access to sensitive information” and expressly encourages businesses to “[c]onsider using multi-factor authentication, such as requiring the use of a password and a code sent by different methods.”<sup>41</sup>
- Emphasizes that companies should respond appropriately when credentials are compromised, providing that businesses should “[r]equire password changes when appropriate—for example, following a breach.”<sup>42</sup>
- Instructs companies to restrict data access privileges by “[s]cal[ing] down access to data” and ensuring that “each employee should have access only to those resources needed to do their particular job.”<sup>43</sup>
- Warns companies that their data security practices depend on their personnel, which “includ[e] contractors” and encourages companies to “investigate [contractor] data security practices and compare their standards” and “verify compliance” with written security expectations.<sup>44</sup>
- Recommends companies encrypt information stored on computer networks, understand their network’s vulnerabilities, and implement policies to correct any security problems and respond to security incidents.<sup>45</sup>

---

<sup>40</sup> *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm’n (Oct. 2016), <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (“The FTC 2016 Guidance”). (last visited Mar. 21, 2025).

<sup>41</sup> *Id.* at 13.

<sup>42</sup> *Id.*

<sup>43</sup> *Id.* at 7.

<sup>44</sup> *Id.* at 27.

<sup>45</sup> *Id.* at 9-11.

- Advises companies not to maintain personal information longer than necessary, not to collect more personal information than necessary, to use industry-tested methods for data security, and monitor and respond to suspicious activity.<sup>46</sup>

64. In 2021, the FTC amended its “Safeguard Rule” that applies to companies that bring together buyers and sellers of products and services.<sup>47</sup> The Safeguard Rule requires covered businesses to “[i]mplement multi-factor authentication for anyone accessing customer information on [the business’s] system,” to “[i]mplement and periodically review access controls [to] [d]etermine who has access to customer information and reconsider on a regular basis whether they still have a legitimate business need for it,” and to “[i]mplement procedures and controls to monitor when authorized users are accessing customer information on your system and detect unauthorized access.”<sup>48</sup>

65. In February 2023, the FTC published an article titled, *Security Principles: Addressing underlying causes of risk in complex systems*. The article highlighted the importance of MFA, stating: “Multi-factor authentication is widely

---

<sup>46</sup> *Id.* at 6-22.

<sup>47</sup> FTC Safeguards Rule, 86 Fed. Reg. 707272-01, 70305-06 (Dec. 9, 2021) (to be codified at 16 C.F.R. § 314.2(h)(2)(i), (xiii)).

<sup>48</sup> *FTC Safeguards Rule: What Your Business Needs to Know*, Fed. Trade Comm’n, <https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know> (last visited Mar. 21, 2025).

regarded as a critical security practice because it means a compromised password alone is not enough to take over someone's account.”<sup>49</sup>

66. The FTC's enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where the FTC has repeatedly obtained MFA as a form of injunctive relief in data security enforcement actions.<sup>50</sup>

67. The FTC has also issued guidance for businesses, like Snowflake and Ticketmaster, regarding how to respond to data breaches, titled *Data Breach Response: A Guide for Business* (the “FTC Response Guidance”). The FTC Response Guidance stresses the importance of providing individuals affected by a data breach with notice, explaining: “If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused.”<sup>51</sup> The guidance emphasizes that businesses should “[c]learly describe what you know about the compromise” and include “what information was taken.”

---

<sup>49</sup> Alex Gaynor, *Security Principles: Addressing underlying causes of risk in complex systems*, Fed. Trade Comm'n (Feb. 1, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems>. (last visited Mar. 21, 2025).

<sup>50</sup> *FTC v. Equifax, Inc.*, No. 1:19-CV-03297, 15 (N.D. Ga. July 23, 2019) (Stipulated Order); *In re Chegg, Inc.*, 2023151 FTC C-4782, 5 (Jan. 25, 2023) (Order); *In re Drizly, LLC*, 2023185 FTC C-4780, 6 (Jan. 9, 2023) (Order).

<sup>51</sup> *Data Breach Response: A Guide for Business*, Fed. Trade Comm'n (Feb. 2021), <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business> (“FTC Response Guidance”). (last visited Mar. 21, 2025).

68. Notifying individuals as to the type of information that was compromised in the breach provides key information that allows them to “take steps to limit the damage.”<sup>52</sup> In particular, if individuals are notified of compromised PCD, they can take steps to prevent credit/debit card fraud losses such as that which Plaintiff and Class Members have had to reimburse to their affected customers.

69. Specific to cloud-storage applications, in June 2020, the FTC published an article titled, *Six steps toward more secure cloud computing*. The article warned, “[a]s cloud computing has become business as usual for many businesses, frequent news reports about data breaches and other missteps should make companies think carefully about how they secure their data.” The article expressly highlights the importance of MFA in protecting sensitive consumer data stored on cloud services, recommending that businesses: “Require multi-factor authentication and strong passwords to protect against the risk of unauthorized access.”<sup>53</sup>

70. In March 2023, the FTC issued a Request for Information seeking public comment on “Business Practices of Cloud Computing Providers that Could

---

<sup>52</sup> *Id.*

<sup>53</sup> Elisa Jillson & Andy Hasty, *Six steps toward more secure cloud computing*, Fed. Trade Comm’n (June 15, 2020), <https://www.ftc.gov/business-guidance/blog/2020/06/six-steps-toward-more-secure-cloud-computing>. (last visited Mar. 21, 2025).

Impact Competition and Data Security.”<sup>54</sup> After reviewing over 100 public comments on the issue, the FTC published a report in November 2023 titled, *Cloud Computing RFI: What we heard and learned*.<sup>55</sup> The report expressly flagged the room for improvement in cloud security as follows: “[A] a number of commenters argued there is a great deal of room for improvement in cloud security; that default security configurations could be better; and that the ‘shared responsibility’ model for cloud security often lacks clarity, which can lead to situations where neither the cloud provider nor the cloud customer implements necessary safeguards.”<sup>56</sup>

**B. Payment Card Industry Data Security Standards were not followed.**

71. The Payment Card Industry Data Security Standards (“PCI DSS”) is an information security standard applicable to the storage of payment card information whose use is mandated by major credit/debit card brands, such as VISA and Mastercard to protect consumers and financial institutions such as Plaintiff and Class Members. The PCI DSS is developed and issued by the

---

<sup>54</sup> *Solicitation for Public Comments on the Business Practices of Cloud Computing Providers*, Fed. Trade Comm’n (Mar. 22, 2023), <https://www.regulations.gov/docket/FTC-2023-0028/document>. (last visited Mar. 21, 2025).

<sup>55</sup> Nick Jones, *Cloud Computing RFI: What we heard and learned*, Fed. Trade Comm’n (Nov. 16, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/cloud-computing-rfi-what-we-heard-learned>. (last visited Mar. 21, 2025).

<sup>56</sup> *Id.* Snowflake used this “shared responsibility” model. *What We Know So Far about the Snowflake “Breach,”* Symmetry Systems (Nov. 6, 2024), <https://www.symmetry-systems.com/blog/what-we-know-so-far-about-the-snowflake-breach/> (“Despite the high-profile nature of the breaches and the potential reputational risk, Snowflake has not deviated from the shared responsibility model.”) (last visited Mar. 21, 2025).

Payment Card Industry Security Standards Council, which describes itself as a “global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.”<sup>57</sup>

72. The PCI DSS applies to companies like Snowflake and Ticketmaster that accept, process, or store credit/debit card information.

73. The PCI DSS reiterates many of the recommendations provided by FTC guidance.

74. As to multifactor authentication, PCI DSS Requirement 8.3 requires: “Secure all non-console administrative access and remote access to the cardholder data environment using multi-factor authentication.”<sup>58</sup>

75. The PCI Security Standards Council has issued an April 2018 supplement to the PCI DSS titled, *PCI SSC Cloud Computing Guidelines*.<sup>59</sup> The PCI Cloud Computing Guidelines again emphasize the importance of MFA, providing: “PCI DSS Requirement 8.2.2 requires multi-factor authentication for all

---

<sup>57</sup> PCI, *Who We Are*, [https://www.pcisecuritystandards.org/about\\_us/](https://www.pcisecuritystandards.org/about_us/) (last visited Mar. 21, 2025).

<sup>58</sup> PCI, *PCI DSS Quick Reference Guide*, 19 (July 2018), [https://listings.pcisecuritystandards.org/documents/PCI\\_DSS-QRG-v3\\_2\\_1.pdf](https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf). See also Frederik Mennes, *PCI DSS 4.0: New multi-factor authentication requirements*, OneSpan (May 23, 2024), <https://www.onespan.com/blog/new-mfa-requirements-in-PCI-DSS-4.0> (noting in requirements 8.4.2 and 8.5 additional configuration for MFA) (last visited Mar. 21, 2025).

<sup>59</sup> PCI Security Standards Council & Cloud Special Interest Group, *PCI SSC Cloud Computing Guidelines* (April 2018), [https://listings.pcisecuritystandards.org/pdfs/PCI\\_SSC\\_Cloud\\_Guidelines\\_v3.pdf](https://listings.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf). (last visited Mar. 21, 2025).

remote network access to the CDE [cardholder data environment], and when public cloud services are part of a Customer's CDE, all such access will be considered remote access and will require multi-factor authentication.”<sup>60</sup>

76. PCI DSS Requirements 7.1 and 7.2 stress the need to restrict data access privileges, requiring businesses to “[l]imit access to system components and cardholder data to only those individuals whose job requires such access” and “[e]stablish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to ‘deny all’ unless specifically allowed.”<sup>61</sup>

77. The PCI SSC Cloud Computing Guidelines includes a section titled *Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)*, which provides: “As the Customer's access to network level data can be severely restricted in cloud environments, the responsibility for tracking intrusions at the network layer will often reside with the Provider, as the only entity that has sufficient privileges to do this across the underlying infrastructure.”<sup>62</sup> The guidelines go on to note that for SaaS providers such as Snowflake: “Since

---

<sup>60</sup> *Id.* at 77.

<sup>61</sup> PCI, *PCI DSS Quick Reference Guide*, *supra* n. 58 at 18-19.

<sup>62</sup> PCI, *PCI SSC Cloud Computing Guidelines*, *supra* n. 59 at 63.

customer access to low-level network traffic is impossible, it must rely on Providers for IDS/IPS, monitoring and alerting.”<sup>63</sup>

78. The PCI DSS includes the following requirements and recommendations that mirror the FTC’s guidance on data retention, data encryption, monitoring data access, and implementing data security policies.<sup>64</sup>

- **Requirement 1.2.** “Build firewall and router configurations that restrict all traffic, inbound and outbound, from “untrusted” networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the cardholder data environment.”
- **Requirement 3.1.** “Limit cardholder data storage and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in your data retention policy. Purge unnecessary stored data at least quarterly.”
- **Requirement 4.** “Encrypt transmission of cardholder data across open, public networks.”
- **Requirement 10.** “Regularly Monitor and Test Networks . . . To prevent exploitation, organizations must regularly monitor and test networks to find and fix vulnerabilities”
- **Requirement 10.6.** “Review [audit] logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.”
- **Requirement 12.1.** “Establish, publish, maintain, and disseminate a security policy; review the security policy at least annually and update when the environment changes.
- **Requirement 12.2.** “Implement a risk assessment process that is performed annually and upon significant changes to the

---

<sup>63</sup> *Id.*

<sup>64</sup> PCI, *PCI DSS Quick Reference Guide*, *supra* n. 58 at 12-16, 21-25.



environment that identifies critical assets, threats, and vulnerabilities, and results in a formal assessment.”

- **Requirement 12.10.** “Implement an incident response plan. Be prepared to respond immediately to a system breach.”

**C. Other standards applicable to cloud storage were not followed.**

79. In addition to the general data security standards described above, several authorities have issued guidance specific to cloud data storage, defining the roles and responsibilities of cloud service providers (like Snowflake) and customers (like Ticketmaster).

80. The Center for Internet Security (“CIS”) is a non-profit organization that develops globally recognized best practices for securing IT systems and data. In March 2022, CIS issued a publication titled, *CIS Controls Cloud Companion Guide* that provided guidance on security best practices for customers using cloud services.<sup>65</sup> The guidance included the following recommendations emphasizing the importance of MFA and revoking access to stale credentials:

- **Disable Dormant Accounts.** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.<sup>66</sup>
- **Establish an Access Revoking Process.** Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts,

---

<sup>65</sup> Center for Internet Security, *CIS Controls Cloud Companion Guide* (Mar. 2022), <https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide>. (last visited Mar. 21, 2025).

<sup>66</sup> *Id.* at 18.

instead of deleting accounts, may be necessary to preserve audit trails.<sup>67</sup>

- **Require MFA for Administrative Access.** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.<sup>68</sup>

81. ISO/IEC 27017 is an international standard that “provides controls and implementation guidance for both cloud service providers and cloud service customers.”<sup>69</sup> Control 9.2.3 specifically highlights that cloud service customers (like Ticketmaster) should use MFA, and cloud service providers (like Snowflake) should provide MFA capabilities as follows<sup>70</sup>:

Cloud service customer	Cloud service provider
The cloud service customer should use sufficient authentication techniques (e.g., multi-factor authentication) for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service according to the identified risks.	The cloud service provider should provide sufficient authentication techniques for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service, according to the identified risks. For example, the cloud service provider can provide multi-factor authentication capabilities or enable the use of third-party multi-factor authentication mechanisms.

<sup>67</sup> *Id.* at 20.

<sup>68</sup> *Id.*

<sup>69</sup> Telecommunication Standardization Sector, *International Standard ISO/IEC 27017*, Int'l Telecomms. Union, 1 (Dec. 15, 2015), <https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027017-2015.pdf>. (last visited Mar. 21, 2025).

<sup>70</sup> *Id.* at 9.

#### **IV. The Data Breach harmed Plaintiff and Class Members.**

82. As soon as NOFFCU received notice from VISA<sup>71</sup> of the debit or credit payment card numbers affected by the Data Breach, NOFFCU investigated the issue, notified its customers and reissued those debit or credit payment cards that were still active. NOFFCU also determined that it had reimbursed customers for debit or credit payment card fraud that likely occurred due to the Data Breach.

83. Upon information and belief, thousands of other credit unions, banks and other financial institutions across the country underwent the same process as Plaintiff.

84. Information protected by credentials—usernames and passwords—is intended to stay private, and not to be disclosed to third parties (otherwise, why password-protect the information, at all?). But because of Defendants' failure to follow basic cybersecurity guidelines, the information stored on Snowflake's cloud-based servers was accessible to cybercriminals, who exfiltrated the data for nefarious purposes.

85. Ticketmaster disclosed that certain types of personal information and PCD were exposed in the Data Breach. Information disclosed included, at a minimum, consumer name, contact information, and credit card information.

---

<sup>71</sup> Ticketmaster has confirmed this information was included in the data breach. Ticketmaster Data Security Incident, <https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident>. (last visited Mar. 21, 2025).

86. The PCD exposed is extremely valuable and can be used for many nefarious purposes.

**A. The Data Breach caused immediate damages to Plaintiff and Class Members.**

87. The Data Breach caused substantial damage to Plaintiff and Class Members, who had to act immediately to mitigate the massive fraudulent transactions being made on payment cards that they had issued to their customers, while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected from most fraud loss, but Plaintiff and Class Members are not. Financial institutions, like Plaintiff and Class Members, bear primary responsibility for reimbursing customers for fraudulent charges on the payment cards they issue and pay for the costs of reissuing payment cards that had to be canceled and reissued as a result of a data breach.

88. As a result of the Data Breach, Plaintiff and Class Members were forced to cancel and reissue payment cards, change or close accounts, notify customers that their payment cards were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on potentially impacted accounts, and take other steps to protect themselves and their customers. Plaintiff and Class Members also lost interest and transaction fees due to reduced card usage. Furthermore, debit and credit cards belonging to Plaintiff

and Class Members—as well as the account numbers on the face of the cards—were devalued.

89. The financial damages suffered by Plaintiff and Class Members due to the Data Breach are massive and continue to increase, affecting millions of accounts.

90. The damages suffered by Plaintiff and Class Members were a foreseeable result of Defendants' failure to protect their customers' personal information and PCD.

## **PART TWO: TICKETMASTER AND LIVE NATION**

### **I. Ticketmaster's business and data security promises.**

91. Consumers are largely unable to purchase concert tickets or enjoy concerts without working through Live Nation, and its wholly owned subsidiary Ticketmaster.

92. Live Nation and Ticketmaster control approximately 70% of the American market for live event ticketing, selling hundreds of millions of tickets

per year.<sup>72</sup> Live Nation reported a quarterly revenue of \$7.7 billion in November 2024.<sup>73</sup>

93. Live Nation considers itself the world's leading live entertainment ticketing sales and marketing company based on the number of tickets sold. In 2023, Ticketmaster distributed over 620 million tickets through [www.ticketmaster.com](http://www.ticketmaster.com), [www.livenation.com](http://www.livenation.com), the companies' mobile apps, and other websites and retail outlets. The same year, Live Nation connected over 765 million individuals to live events.<sup>74</sup>

94. Live Nation and Ticketmaster are highly integrated with respect to collecting customer personal information, sharing customer personal information, and developing and implementing privacy policies. To provide several examples, near the time of the Data Breach:

- When a consumer purchases tickets through Live Nation, they are often informed the purchase is “powered by Ticketmaster” or redirected to a Ticketmaster purchasing portal.
- Live Nation and Ticketmaster maintain similar privacy policies that list the following identical Live Nation point of contact for consumers with privacy inquiries: Attention: Privacy Officer,

---

<sup>72</sup> Daniel Allen, *Does Live Nation Own Ticketmaster? The Complete Story Behind Entertainment's Biggest Merger*, The Ticket Lover (Oct. 28, 2024), <https://theticketlover.com/does-live-nation-own-ticketmaster/> (last visited Mar. 21, 2025).

<sup>73</sup> Live Nation, *LIVE NATION ENTERTAINMENT REPORTS THIRD QUARTER 2024 RESULTS* (Nov. 11, 2024), <https://www.livenationentertainment.com/2024/11/live-nation-entertainment-reports-third-quarter-2024-results/>. (last visited Mar. 21, 2025).

<sup>74</sup> Live Nation, 2024 Annual Report (Form 10-K) at 2 (Feb. 22, 2024), <https://investors.livenationentertainment.com/sec-filings/annual-reports/content/0001335258-24-000017/0001335258-24-000017.pdf>. (last visited Mar. 21, 2025).

Legal, Live Nation Entertainment, Inc., 9348 Civic Center Drive, Beverly Hills, CA 90210.<sup>75</sup>

- Live Nation’s Privacy Policy discloses: “We will share information within the Live Nation family of companies. This may include Ticketmaster and Live Nation-owned or operated venues, for example.”<sup>76</sup>
- Ticketmaster’s Privacy Policy likewise discloses that customer data will be shared “[w]ithin the Ticketmaster group” and directs consumers to write to Live Nation’s corporate address with privacy inquiries.<sup>77</sup>

95. Ticketmaster requires consumers who purchase tickets on their platform to provide their personal information to Ticketmaster, both to facilitate ticket sales and for Ticketmaster’s own business purposes. Ticketmaster promises to keep consumers’ personal information secure and does not allow consumers to opt out of sharing their personal information.

96. Ticketmaster made express commitments to protecting consumer personal information in its Privacy Policy, assuring consumers in a caption titled, *Looking After Your Information*, “We have security measures in place to protect your information.”<sup>78</sup>

---

<sup>75</sup> Compare Live Nation Entertainment, *Privacy Policy* (“Live Nation, *Privacy Policy*”), <https://web.archive.org/web/20240222185813/https://help.livenation.com/hc/en-us/articles/10464047306641-Live-Nation-Entertainment-Privacy-Policy> (archived Feb. 22, 2024), with Ticketmaster, *PRIVACY POLICY* (“Ticketmaster, *Privacy Policy*”), *Contact Us*, <https://web.archive.org/web/20240226041015/https://privacy.ticketmaster.com/privacy-policy#contact-us> (archived Feb. 26, 2024) (last visited Mar. 21, 2025).

<sup>76</sup> Live Nation, *Privacy Policy*, *supra* n. 15975.

<sup>77</sup> Ticketmaster, *Privacy Policy*, *supra* n. 75.

<sup>78</sup> *Id.*

97. Ticketmaster publicly represented that data security forms a crucial aspect of its business model. For instance, on a segment of Ticketmaster LLC’s website, the company stated:

“Our goal is to maintain your trust and confidence by handling your personal information with respect and putting you in control.”<sup>79</sup>

“As a global company, our fans are located all over the world, depending on your market there are specific laws and regulations around privacy rights such as the GDPR in Europe, LGPD in Brazil and CCPA in United States.”<sup>80</sup>

“We have security measures in place to protect your information.”<sup>81</sup>

98. Live Nation also maintained a privacy policy section, affirming its adherence to various state and federal laws.<sup>82</sup>

99. Ticketmaster’s Privacy Policy includes specific commitments relating to “Data Transfers,” which provides as follows<sup>83</sup>:

When transferring information, there are strict rules in place to ensure your data is still protected to the highest standard. Where we do this, we will ensure that appropriate safeguards are put in place. Where your information is transferred outside of your local market, we use contractual measures and internal mechanisms requiring the recipient to comply with the privacy standards of the exporter[.]

---

<sup>79</sup> *Id.*

<sup>80</sup> *Id.*

<sup>81</sup> *Id.*

<sup>82</sup> Live Nation, *Privacy Policy*, *supra* n. 75.

<sup>83</sup> *Id.*



100. Ticketmaster maintains a website captioned, *Our Commitments*, which make the following representations concerning privacy (the “Privacy Commitments”)<sup>84</sup>:

- **Fair & Lawful.** We comply with all applicable data protection laws and listen to your expectations when it comes to how your information is handled.
- **Security & Confidentiality.** The security of our fans’ information is a priority for us. We take all necessary security measures to protect personal information that’s shared and stored with us.
- **Third Parties & Partners.** We work with our partners to put on amazing live events and provide additional services that we think you’ll love. We always ask them to maintain the same standards of privacy.
- **Privacy By Design.** We embed privacy in the development of our products and services to ensure that we always respect your personal information.
- **Storage & Retention.** We store and use your data only as long as we need to, from complying with our legal obligations to making sure you know when your favorite artist is on tour.

101. Ticketmaster represented on a separate FAQ website that it complies with the PCI DSS and that it “take[s] compliance very seriously.”<sup>85</sup>

---

<sup>84</sup> Ticketmaster, *Our Commitments*, <https://web.archive.org/web/20230517182539/https://privacy.ticketmaster.com/our-commitments> (archived May 17, 2023) (“Privacy Commitments”) (last visited Mar. 21, 2025).

<sup>85</sup> Ticketmaster Business, *Define the Future of Live with Us*, [https://web.archive.org/web/20240319080146/https://business.ticketmaster.com/web/20240319080146/https://business.ticketmaster.com/](https://web.archive.org/web/20240319080146/https://business.ticketmaster.com/web/20240319080146/https://business.ticketmaster.com/web/20240319080146/https://business.ticketmaster.com/) (archived Mar. 19, 2024) (last visited Mar. 21, 2025).

102. Ticketmaster relies on multiple third-party service providers to carry out key business functions including payment processing, marketing, customer service, and data storage.<sup>86</sup>

103. At the same time, Ticketmaster states that it is “committed to being the safest, most reliable ticket marketplace in the world.”<sup>87</sup> Ticketmaster recommended to consumers that they could take several steps to secure their online accounts:

- “Make sure you’re using a strong password for your account. Your password should be unique to your Ticketmaster account, and therefore not used for any other accounts (banking, retail sites, email, etc). You can easily reset your password if you need to.”<sup>88</sup>
- “Another good way to protect your tickets is to make sure the phone number associated with your Ticketmaster account is up to date. For extra security during a ticket purchase, you may also be asked to authenticate your account by inputting a code sent to your phone number.”<sup>89</sup>
- “Just like you want to make sure your Ticketmaster password is unique, you should do the same for your personal email. Make sure you’re using a strong, unique password there, too. If your email gets hacked, which unfortunately does happen, it could

---

<sup>86</sup> Ticketmaster, *Privacy Policy: Who We Share Your Data With & Why*, <https://web.archive.org/web/20240219050226/https://privacy.ticketmaster.com/privacy-policy#who-we-share-your-data-with-&-why> (archived Feb. 19, 2024) (last visited Mar. 21, 2025).

<sup>87</sup> Ticketmaster, *How to Secure Your Account and Protect Your Tickets* (Apr. 12, 2024), <https://web.archive.org/web/20240426053554/https://blog.ticketmaster.com/account-security-tips-password-protect-tickets/>. (last visited Mar. 21, 2025).

<sup>88</sup> *Id.*

<sup>89</sup> *Id.* In other words, Ticketmaster suggested to consumers that they could keep their account safe by enabling MFA.

allow bad actors to use it to try to gain access to your Ticketmaster account.”<sup>90</sup>

- But be aware of scammers sharing fake information about Ticketmaster, including fake customer service phone numbers that appear in search engines.<sup>91</sup>

104. While Ticketmaster told consumers that *they* should take multiple steps to keep their personal information secure, because Ticketmaster used third-party service providers to maintain personal information (and to employ the same data privacy standards as those employed by Ticketmaster),<sup>92</sup> Ticketmaster’s customers actually had no way to keep their information safe—even following the steps above—if Ticketmaster and its service providers were not taking the most basic steps to secure consumer information.

105. Ticketmaster is a Snowflake customer. Ticketmaster stores the personal information of its consumers on Snowflake’s Data Cloud services, which include customers’ names, addresses, contact information (email and phone numbers), and payment card information.

106. Ticketmaster did not employ rudimentary security measures that were available to it through Snowflake, including implementing a policy mandating that its users employ MFA on their accounts.

---

<sup>90</sup> *Id.*

<sup>91</sup> *Id.* In other words, Ticketmaster warned consumers that they could fall prey to phishing schemes.

<sup>92</sup> Ticketmaster, *Our Commitments*, *supra* n. 16884.

**II. Ticketmaster owed a duty of care to Plaintiff and Class Members.**

107. Ticketmaster agrees to accept debit/and credit cards in order to be paid for its services for its customers.

108. As a condition of purchasing a ticket from Ticketmaster, consumers provide their personal information to Ticketmaster, including their names, contact information, and payment card information such as credit card number and expiration date.

109. To collect and store personal information and PCD of consumers, Ticketmaster must comply with the PCI DSS to prevent the dissemination of that information.

110. Ticketmaster owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the personal information and PCD in Snowflake's possession from being compromised, accessed, stolen, or misused by unauthorized parties.

111. Ticketmaster owed a common law duty to Plaintiff and Class Members to supervise Snowflake in the collection, storage, and security of Plaintiff's and Class Members' customers' personal information.

112. Ticketmaster's duty of reasonable care is established by governmental regulations and industry guidance establishing industry standards for data security to safeguard personal information stored on cloud platforms, as described herein.

113. Ticketmaster owed a statutorily imposed duty to refrain from unfair and deceptive practices.

114. Ticketmaster understood that it owed a duty of care to Plaintiff and Class Members under the PCI DSS as well as other applicable laws and industry standards.

115. This duty extended to Ticketmaster's oversight of any third-parties or vendors to which it entrusted its customers' personal information. On February 22, 2024, Live Nation, in its SEC Annual Report, explicitly identified data security as a risk facing the business, and stated as follows<sup>93</sup>:

Due to the nature of our business, we process, store, use, transfer and disclose certain personal or sensitive information about our customers and employees. Penetration of our network or other misappropriation or misuse of personal or sensitive information and data, including credit card information and other personally identifiable information, could cause interruptions in our operations and subject us to increased costs, litigation, inquiries and actions from governmental authorities, and financial or other liabilities. In addition, security breaches, incidents or the inability to protect information could lead to increased incidents of ticketing fraud and counterfeit tickets.

. . . .

We also face risks associated with security breaches and incidents affecting third parties with which we are affiliated or with which we otherwise conduct business. In particular, hardware, software or applications we develop or procure from third parties may contain, and have contained, defects in design or manufacture and/or may pose a

---

<sup>93</sup> Live Nation, 2024 Annual Report (Form 10-K) at 17-18 (Feb. 22, 2024), <https://investors.livenationentertainment.com/sec-filings/annual-reports/content/0001335258-24-000017/0001335258-24-000017.pdf>. (last visited Mar. 21, 2025).

security risk that could unexpectedly compromise information security, but none of which have been material to date.

116. Ticketmaster knew or should have known of the importance of oversight related to third-party providers. In 2018, Ticketmaster announced a data breach incident of a provider of AI-powered live chat widgets, which Ticketmaster was deploying on localized sites across the world.<sup>94</sup> The Data Breach was thus foreseeable because Ticketmaster previously dealt with a data breach involving a third-party provider which did or reasonably should have put Ticketmaster on notice of its duty in reasonably selecting and overseeing third-party vendors it entrusted with customers' personal information.

### **III. Ticketmaster breached its duty to protect PCD and personal information.**

117. Despite Ticketmaster's explicit assurances that it would employ reasonable measures to safeguard its customers' sensitive personal information, including PCD, and only share that information with expressly authorized individuals, an "unauthorized" person or persons accessed Ticketmaster's network servers and reportedly stole the personal information they found.

---

<sup>94</sup> Catalin Cimpanu, *Ticketmaster Announces Data Breach Affecting 5% of All Users*, BleepingComputer (June 17, 2018), <https://www.bleepingcomputer.com/news/security/ticketmaster-announces-data-breach-affecting-5-percent-of-all-users/>. (last visited Mar. 21, 2025).

118. Live Nation played a primary role in investigating the Data Breach, disclosing in a Form 8-K filing to the U.S. Securities and Exchange Commission filed on May 31, 2024:

On May 20, 2024, Live Nation Entertainment, Inc. (the “Company” or “we”) identified unauthorized activity within a third-party cloud database environment containing Company data (primarily from its Ticketmaster L.L.C. subsidiary) and launched an investigation with industry-leading forensic investigators to understand what happened. On May 27, 2024, a criminal threat actor offered what it alleged to be Company user data for sale via the dark web. We are working to mitigate risk to our users and the Company, and have notified and are cooperating with law enforcement. As appropriate, we are also notifying regulatory authorities and users with respect to unauthorized access to personal information.”<sup>95</sup>

119. Several months after the Data Breach, on June 8, 2024, Ticketmaster disclosed the Data Breach to consumers in a notice.

120. In the Ticketmaster Notice, Ticketmaster represented that the Data Breach occurred between April 2, 2024, and May 18, 2024, and that Ticketmaster had determined personal information was affected on May 23, 2024.

121. Ticketmaster also recommended that recipients “take steps to protect against identity theft and fraud,” offered 1 year of free credit monitoring services, and made numerous additional recommendations to guard against identity fraud including:

---

<sup>95</sup> Live Nation Entertainment, Inc., Current Report (Form 8-K) (May 20, 2024), <https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm>. (last visited Mar. 21, 2025).

[W]e recommend you remain vigilant and take steps to protect against identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for signs of suspicious activity. To further protect your identity and as a precaution, we are also offering you identity monitoring with TransUnion at no cost to you. Identity monitoring will look out for your personal data on the dark web and provide you with alerts for 1 year from the date of enrollment if your personally identifiable information is found online. . . .

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. . . .

You should remain vigilant for incidents of fraud or identity theft by reviewing account statements and monitoring free credit reports. When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. You should also call your local police department and file a report of identity theft. Finally, you should make sure to keep a copy of the police report in case you need to provide it to creditors or credit reporting agencies when accessing or disputing inaccurate information. . . .

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze.<sup>96</sup>

122. However, Ticketmaster was vague as to the types of personal information compromised in the Data Breach and the number of affected consumers. The “Ticketmaster Data Security Incident” webpage describing the

---

<sup>96</sup> Ticketmaster Data Security Incident, <https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident> (last visited Mar. 21, 2025).



Data Breach disclosed that it discovered “unauthorized activity on an isolated cloud database hosted by a third-party data services provider” and that the “database contained limited personal information of some customers who bought tickets to events in North America . . . . [which] may include email, phone number, encrypted credit card information as well as some other personal information provided to us.”<sup>97</sup> Neither the Ticketmaster Notice nor Ticketmaster Data Security Incident webpage included any additional detail on the types of credit card information taken, nor did they include details as to the number of total affected customers. And the Ticketmaster Notice was untimely, coming several months after the Data Breach.

123. At the time of the Data Breach, Ticketmaster failed to maintain reasonable data security measures and comply with FTC guidance, the PCI DSS, and other relevant industry standards summarized above. These data security failings included:

- Ticketmaster did not enforce MFA for its Snowflake accounts. Indeed, Ticketmaster chose to use Snowflake to store the personal information of millions of its customers despite knowing that Snowflake did not allow customers to enforce MFA.
- Ticketmaster did not rotate or disable the credentials of old Snowflake accounts.

---

<sup>97</sup> *Id.*

- Ticketmaster did not implement network allowed lists that restricted Snowflake account access to certain locations or trusted users.

124. In order to utilize PCD from Plaintiff and the Class to pay for its goods and services, Ticketmaster must follow the Payment Card Industry Data Security Standards (“PCI DSS”), a list of 12 information security requirements that were promulgated by the Payment Card Industry Security Standards Council.

125. The PCI DSS list applies to all organizations that store, process or transmit cardholder data. PCI DSS requires merchants like Ticketmaster to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

126. The 12 requirements of the PCI DSS are:

**Build and Maintain a Secure Network**

- (1) Install and maintain Network Security Controls
- (2) Apply Secure Configurations to All Systems

**Protect Account Data**

- (3) Protect Stored Account Data
- (4) Protect Cardholder Data with Strong Cryptology During Transmission Over Open, Public Networks

### **Maintain a Vulnerability Management Program**

- (5) Protect All Systems and Networks from Malicious Software
- (6) Develop and Maintain Secure Systems and Software

### **Implement Strong Access Control Measures**

- (7) Restrict Access to System Components and Cardholder Data by Business Need to Know
- (8) Identify Users and Authenticate Access to System Components
- (9) Restrict Physical Access to Cardholder Data

### **Regularly Monitor and Test Networks**

- (10) Log and Monitor All Access to System Components and Cardholder Data
- (11) Test Security of Systems and Networks Regularly

### **Maintain an Information Security Policy**

- (12) Support Information Security with Organizational Policies and Programs.<sup>98</sup>

---

<sup>98</sup> PCI Security Standards Council, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 4.0.1* (June 2024), [https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4\\_0\\_1.pdf](https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf). Note, the PCI DSS was updated from v4.0 to v4.0.01 in June of 2024, but none of the substantive requirements changed with this update, so the duties imposed applied prior to the time of the Data Breach. PCI Security Standard Council, *Payment Card Industry Data Security Standard Summary of Changes from PCI DSS Version 4.0 to 4.0.1* (June 2024), <https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4-0-to-v4-0-1-Summary-of-Changes-r1.pdf>.

127. Ticketmaster's obligations under the Payment Card Industry Data Security Standard v4.0.1 include the implementation of robust security measures to safeguard sensitive payment card data. PCI DSS establishes a comprehensive framework that mandates adherence to twelve high-level requirements, several of which are particularly relevant to the deficiencies alleged in this case.

128. As alleged in this Complaint, Ticketmaster failed to comply with the following PCI DSS, Encryption with strong cryptographic methods, Requirement 3; Requirement 3.2, Storage of account data is kept to a minimum; Access Controls, Requirement 8; Logging and Monitoring Requirements, Requirement 10; and Third-Party Documentation and Compliance Validation, Requirement 12.8.

129. The Data Breach exposed Ticketmaster's improper collection and maintenance of PCD going as far back as 2009, which clearly violated PCD DSS.

130. In addition, under the PCI DSS Ticketmaster's duty of care included overseeing Snowflake as a third-party processor to ensure that Snowflake adhered to the Payment Card Industry Data Security Standard requirements and other data protection mandates.

131. Ticketmaster failed to take these actions despite its parent company, Live Nation, explicitly reporting that it faced data security risks just two months prior.

132. Ticketmaster further failed to properly investigate, retain, oversee and audit a competent cloud-based data storage provider, because Snowflake similarly had numerous data security failings, as described herein.

133. Ticketmaster's data security failings enabled the Data Breach. Without these basic protections, UNC5537 was able to exfiltrate the personal information of over 560 million Ticketmaster consumers with nothing more than stolen Ticketmaster Snowflake credentials obtained through malware campaigns—and traffic the data to other cybercriminals.

134. Ticketmaster's failings were particularly egregious given the enormous amount of personal information it stored on Snowflake's servers. Tasked with handling the data of over 560 million consumers, Ticketmaster's failure to implement basic data security measures is all the more inexplicable and reckless.

135. Indeed, each of these basic protections could have prevented the Data Breach. For example:

- Had Ticketmaster implemented MFA, UNC5537 would not have been able to access Ticketmaster's data with just stolen credentials. MFA would have required an additional layer of authentication (i.e., a code sent via text message or email) that UNC5537 would not have had access to.
- Ticketmaster could have also prevented the Data Breach by maintaining a policy of rotating or disabling credentials that were either old or compromised in other data breaches. As the Mandiant Report found that a "majority of the credentials used by UNC5537" were available from historic malware campaigns dating back to 2020, a policy that disabled previously-

compromised credentials could have prevented the Data Breach.<sup>99</sup>

- Ticketmaster could have also prevented the Data Breach by maintaining stricter network allow lists that restricted access to customer personal information to certain locations or trusted user accounts that were not previously compromised.

136. In addition, Ticketmaster ignored the FTC Response Guidance by failing to give affected consumers sufficient information regarding the scale of the attack and the types of information taken in the Ticketmaster Notice.<sup>100</sup>

137. Ticketmaster, through these basic data security failings, breached its express representations in its Privacy Policy and Commitments. These representations included but were not limited to, statements that Ticketmaster had implemented “security measures in place to protect [consumers’] information,” would “ensure [consumers’] data was protected to the highest standard,” and would “take all necessary security measures to protect personal information that’s shared and stored with us.”

138. In the alternative, Ticketmaster breached implied commitments to protect consumer personal information by virtue of mandating that consumers provide their sensitive personal information as a condition of purchase.

139. Ticketmaster’s basic data security failings also breached its duty of care to protect the personal information and PCD of consumers.

---

<sup>99</sup> *Mandiant Report*, *supra* n. 19.

<sup>100</sup> FTC Response Guidance, *supra* n. 51.

**IV. The PCD and personal information of Plaintiff's and Class Members' customers was stolen.**

140. At a minimum, the stolen personal information about Ticketmaster customers included the identifiers disclosed in the Ticketmaster Notice, which informed customers that the information exposed in the Data Breach “may include email, phone number, encrypted credit card information as well as some other personal information provided to us.”<sup>101</sup>

141. The stolen personal information also included names, addresses, emails, and phone numbers of Ticketmaster customers, as well as information regarding tickets they purchased through Ticketmaster, order confirmation details, and credit card information such as the last four digits of their payment cards and expiration dates. On May 28, 2024, around the time of the Data Breach, this very information was advertised for sale on a dark web forum post by a cybercriminal group by the name of “ShinyHunters” that claimed the information was stolen in the Snowflake Data Breach. A screenshot of this post is provided below.<sup>102</sup>

---


<sup>101</sup> Ticketmaster, *Ticketmaster Data Security Incident*, <https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident> (last visited Mar. 24, 2025)

<sup>102</sup> Lawrence Abrams, *Ticketmaster confirms massive breach after stolen data for sale online*, Bleeping Computer (May 31, 2024), <https://www.bleepingcomputer.com/news/security/ticketmaster-confirms-massive-breach-after-stolen-data-for-sale-online/>. (last visited Mar. 24, 2025).

**Live Nation / Ticketmaster 560M Users + Card Details 1.3TB**  
by ShinyHunters - Tuesday May 28, 2024 at 06:02 PM

05-28-2024, 06:02 PM #1

**[Owner] ShinyHunters**



**Live Nation / TicketMaster**

**Data includes**  
560 million customers full details (name, address, email, phone)  
Ticket sales, event information, order details.  
CC detail - customer, last 4 of card, expiration date.  
customer fraud details  
much more

**Price is \$500k USD. One time sale.**

**Folder / Table Size**

Folder	size
390G	./processed
149G	./csv
47G	./sales_ord_deluxe_hdr/3
49G	./sales_ord_deluxe_hdr/7
48G	./sales_ord_deluxe_hdr/4
44G	./sales_ord_deluxe_hdr/5
43G	./sales_ord_deluxe_hdr/8
47G	./sales_ord_deluxe_hdr/2
46G	./sales_ord_deluxe_hdr/9

**ADMINISTRATOR**

Posts: 31  
Threads: 7  
Joined: May 2023  
Reputation: 1,187

142. While Ticketmaster represented in its Notice that the stolen credit card information was “encrypted,” developments following the Data Breach call the veracity of Ticketmaster’s statements into question.

143. For example, in December 2024, Visa issued over a hundred Compromised Account Management System (“CAMS”) alerts to several credit unions. The CAMS alerts linked to a Ticketmaster press release and indicated that the breach compromised unique payment card numbers, along with data related to the payment card issuer and the cardholder account. In all, the CAMS alerts identified over a thousand payment cards compromised by the Data Breach. These CAMS alerts, together with Plaintiff’s allegations of attempted fraud and payment



card misuse, demonstrate that Ticketmaster’s representations concerning the Data Breach may very well be confusing, incorrect, or blatantly misleading.<sup>103</sup>

144. In addition, the Data Breach compromised information relating to tickets purchased through Ticketmaster, which can also be used to perpetrate identity fraud. For example, as a threat, the cybercriminals leaked data for upcoming popular concerts and events that allowed fraudsters to effectively steal the ticket from a paying customer.<sup>104</sup>

### **PART THREE: SNOWFLAKE**

145. Snowflake is aware and understands that data security is a key feature of the data storage services that it provides to its customers. The following examples illustrate how Snowflake’s marketing highlights the strength of its data security practices as a selling point to its customers:

- Snowflake maintains a “Security Hub” webpage that centralizes updates relating to data security. The header of the Security Hub website provides: “Security has been foundational to the Snowflake platform since the very beginning. Our robust security

---

<sup>103</sup> To the extent that Plaintiff discovers that Ticketmaster’s representations were inaccurate through discovery, it will respectfully seek leave to amend its complaint.

<sup>104</sup> Lawrence Abrams, *Hackers leak 39,000 print-at-home Ticketmaster tickets for 154 events*, Bleeping Computer (July 8, 2024), <https://www.bleepingcomputer.com/news/security/hackers-leak-39-000-print-at-home-ticketmaster-tickets-for-154-events/>; Jonathan Limehouse, *Scammers are accessing Ticketmaster users’ email accounts, stealing tickets, company says*, USA Today (Oct. 1, 2024), <https://www.usatoday.com/story/entertainment/music/2024/10/01/ticketmaster-scammers-disappearing-tickets/75470713007/>. (last visited Mar. 24, 2025).

features help you protect your data so you can achieve the results you need.”<sup>105</sup>

- The Security Hub website also includes the following quote from Brad Jones, Snowflake’s Chief Information Security Officer (“CISO”), emphasizing Snowflake’s “industry-leading” data security policies: “Since our founding in 2012, the security of our customers’ data has been our highest priority. This unwavering commitment is why we’re continuously strengthening our industry-leading, built-in security policies to deliver a trusted experience for our customers. To foster ongoing transparency, we will regularly update this page with the latest security information.”<sup>106</sup>
- Snowflake also maintains a “Securing Snowflake” website that provides customers with data security guidance. The website represents, “Snowflake provides industry-leading features that ensure the highest levels of security for your account and users, as well as all the data you store in Snowflake.”<sup>107</sup>

146. Snowflake is also well aware of industry guidance and regulations that set standards for effective data security practices. Snowflake’s marketing repeatedly advertises that its “industry-leading” data security practices enable companies to comply with relevant data security standards and regulations.

147. For example, on a webpage titled “Data Security Compliance: Protecting Sensitive Data” (the “Data Security Compliance website”), Snowflake represents: “Snowflake helps organizations streamline security compliance,

---

<sup>105</sup> Snowflake, *Snowflake Security Hub*, <https://www.snowflake.com/en/resources/learn/snowflake-security-hub/> (last visited Mar. 21, 2025).

<sup>106</sup> *Id.*

<sup>107</sup> Snowflake, *Securing Snowflake*, <https://docs.snowflake.com/en/guides-overview-secure> (last visited Mar. 21, 2025).

providing the tools and support required to meet regulatory compliance standards. With industry-leading data security and governance features, organizations can shift their focus from protecting their data to analyzing it.”<sup>108</sup>

148. Snowflake advertises that it is a Level 1 service provider, compliant with PCI DSS.<sup>109</sup> Thus, it was aware of MFA being the industry standard for storage of PCD yet failed to require it.<sup>110</sup>

149. On the Data Security Compliance website, Snowflake further represents how its services enable customers to comply with relevant industry standards and regulations, touting that its services afford customers “[b]aked-in government and industry data security compliance” and allow for “comprehensive compliance, security and privacy controls that are universally enforced.” For example, in a section titled, “How Snowflake Supports Security Compliance,” Snowflake represents the following<sup>111</sup>:

- **“Baked-in government and industry data security compliance.** Snowflake has achieved numerous government and industry data security compliance credentials, validating the high level of security required by industries, as well as state and federal governments. Snowflake’s government deployments have achieved Federal Risk and Authorization Management Program (FedRAMP) Authorization to Operate (ATO) at the Moderate level along, and support a range of compliance

---

<sup>108</sup> Snowflake, *Data Security Compliance: Protecting Sensitive Data*, <https://www.snowflake.com/trending/data-security-compliance/> (last visited Mar. 21, 2025).

<sup>109</sup> <https://docs.snowflake.com/en/user-guide/cert-pci-dss>. (last visited Mar. 21, 2025).

<sup>110</sup> <https://listings.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf> (last visited Mar. 21, 2025).

<sup>111</sup> *Id.*

standards: International Traffic in Arms Regulations (ITAR), System and Organization Controls 2 (SOC 2) Type II, PCI DSS and Health Information Trust Alliance (HITRUST).”

- “**Universal governance.** Inconsistent governance policies across systems and users can introduce security risk to your data. Snowflake’s single governance model provides comprehensive compliance, security and privacy controls that are universally enforced. Snowflake Horizon unifies and extends data governance resources. With Snowflake Horizon, data teams, data governors and data stewards can leverage a built-in, unified set of compliance, security, privacy, interoperability and access capabilities in the AI Data Cloud. Snowflake Horizon provides the toolkit required to protect and audit data, apps and models with data quality monitoring and lineage. And advanced privacy policies and data clean rooms allow organizations to tap into the full value of their most sensitive data.”

150. As one of the nation’s largest cloud storage data providers, Snowflake knew or should have known about the importance of implementing effective data security practices to protect personal information stored on the Data Cloud, particularly because it held itself out as doing exactly that.

151. Indeed, cloud storage databases are prime targets for cybercriminals due to the sheer volume of valuable and sensitive data they house. One recent report has highlighted the risks presented by cloud storage as follows<sup>112</sup>:

It is estimated that more than 60% of the world’s corporate data is stored in the cloud. That makes the cloud a very attractive target for hackers. In 2023, over 80% of data breaches involved data stored in the cloud. That is not just because the cloud is an attractive target. In many cases, it is also an easy target due to cloud misconfiguration – that is, companies unintentionally

---

<sup>112</sup> Stuart Madnick, *Why Data Breaches Spiked in 2023*, Harv. Bus. Rev. (Feb. 19, 2024), <https://hbr.org/2024/02/why-data-breaches-spiked-in-2023>. (last visited Mar. 21, 2025).

misuse the cloud, such as allowing excessively permissive cloud access, having unrestricted ports, and using unsecured backups

152. Snowflake knows that it is a high-value target for cybercriminals. In March 2023, the FTC sought comments from Computing Providers (like Snowflake) and their impact on end users, customers, companies, and other businesses across the economy (like Ticketmaster) on the business practices of cloud computing providers including issues related to the market power of these companies, impact on competition, and potential security risks.<sup>113</sup>

**I. Snowflake had a duty to safeguard Plaintiff's and Class Members' information.**

153. Snowflake exists because companies need a company to safeguard their information. Plaintiff's and Class Members' PCD was stored on Snowflake's Data Cloud at the time of the Data Breach by Ticketmaster, with whom Snowflake maintained a business relationship to provide data cloud storage services.

154. Snowflake owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PCD in Snowflake's possession from being compromised, accessed, stolen, or misused by unauthorized parties.

---

<sup>113</sup> Press Release, Fed. Trade Comm'n, *FTC Seeks Comment on Business Practices of Cloud Computing Providers that Could Impact Competition and Data Security* (March 22, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-seeks-comment-business-practices-cloud-computing-providers-could-impact-competition-data>. (last visited Mar. 21, 2025).

155. Because Snowflake’s business is to provide secure cloud data services and store massive amounts of data, including Plaintiff’s and Class Members’ customers’ personal information and PCD, reasonable care is needed because of the highly sensitive and confidential nature of the information it is hired to protect.

156. Snowflake had a duty to exercise reasonable care in safeguarding Plaintiff’s and Class Members’ PCD and personal information because it was reasonably foreseeable that the failure to do so would cause them significant injury.

157. Snowflake’s duty of reasonable care is also set forth in governmental regulations and industry guidance establishing industry standards for data security to safeguard personal information and PCD stored on cloud platforms.

158. Snowflake’s duty of reasonable care is established by its own marketing statements, which hold out its cloud services as providing “built-in,” “baked-in,” “industry leading and otherwise turnkey data and state-of-the-art security compliance systems.”

## **II. Snowflake delayed notification and denied responsibility for its negligent security failures.**

159. After the Data Breach was made public, Snowflake denied that it had any responsibility and instead provided misleading information to cover up how the Data Breach occurred. For example, Snowflake’s Chief Information Security Officer (CISO) Brad Jones stated: “We have not identified evidence suggesting

this activity was caused by a vulnerability, misconfiguration, or breach of Snowflake’s platform” after reviewing threat activity going back to mid-April.<sup>114</sup>

160. Snowflake’s hired cybersecurity investigator Mandiant further obscured Snowflake’s role in the Data Breach by placing sole and complete blame on Snowflake’s customers. Its Chief Technology Officer (CTO) Charles Carmakal claimed: “Based on our investigations to date, a threat actor likely obtained access to multiple organizations’ Snowflake tenants by using credentials stolen by info stealing malware.”<sup>115</sup>

161. Rather than take responsibility for its actions, Snowflake foisted the blame and responsibility onto its customers, such as Ticketmaster, to “query for unusual activity and conduct further analysis to prevent unauthorized user access.”<sup>116</sup>

162. Even after the Data Breach, Snowflake insists that it was not breached. Despite failing to implement many basic cybersecurity measures, which could have prevented the Data Breach, and despite adopting a “shared

---

<sup>114</sup> *Snowflake customers caught in identity-based attack spree*, Cybersecurity Dive (June 3, 2024), <https://www.cybersecuritydive.com/news/snowflake-customer-databases-breached/717801/>. (last visited Mar. 21, 2025).

<sup>115</sup> *Id.*

<sup>116</sup> Alert, *Snowflake Recommends Customers Take Steps to Prevent Unauthorized Access*, CISA (June 3, 2024), <https://www.cisa.gov/news-events/alerts/2024/06/03/snowflake-recommends-customers-take-steps-prevent-unauthorized-access>. (last visited Mar. 21, 2025).

responsibility” model, Snowflake insisted that it was not responsible. Snowflake’s CEO Sridhar Ramaswamy made such representations to investors:

We obviously had some rough headlines in the quarter as some of our customers dealt with cybersecurity threats. As extensively reported, the issue wasn't on the Snowflake site. After multiple investigations by internal and external cybersecurity experts, we found no evidence that our platform was breached or compromised. However, we understand that when it comes to cybersecurity, we are all in it together.

My one ask of all businesses around the world, whether they are a Snowflake customer or not, is to enable and enforce multi-factor authentication in your organization and ensure that you have network policies that are as strong as possible. Two things we at Snowflake have supported since 2016.<sup>117</sup>

### **III. Snowflake’s negligence as a sophisticated cloud-storage services provider.**

163. As a major cloud storage services provider, and business associate and/or vendor of Ticketmaster, which handles personal information and PCD, Snowflake has a duty to implement adequate data security systems, protocols, and practices to protect the financial and personal information it contracts to store from known vulnerabilities and maintain a security system consistent with relevant industry standards.

---

<sup>117</sup> *Snowflake Inc. (SNOW) Q2 2025 Earnings Call Transcript* (Aug. 21, 2024), <https://seekingalpha.com/article/4716334-snowflake-inc-snow-q2-2025-earnings-call-transcript>. (last visited Mar. 21, 2025).



164. Snowflake is also responsible for other significant violations of the standard of care for data protection by cloud storage entities. These include, but are not limited to:

- a. Failing to mandate that its clients, like Ticketmaster, enable MFA.  
Its security model placed the burden on Snowflake's clients to enable MFA but did not enforce it, leaving accounts vulnerable.
- b. Failing to proactively monitor for credential abuse. Mandiant reports that 79.7% of affected accounts had previously exposed credentials.
- c. Failing to require that its clients, like Ticketmaster, regularly rotate their passwords.
- d. Failing to monitor for leaked credentials of its own employees and its clients' employees on the dark web.
- e. Failing to require its clients to restrict access to trusted IP addresses.
- f. Failing to require that its clients disable inactive accounts to reduce risk.

165. Snowflake's negligent failures were substantial factors contributing to this massive breach. Snowflake, as a vendor to Ticketmaster, acted as their

business associate. Therefore, Snowflake and Ticketmaster are therefore jointly and severally liable for causing injury to Plaintiff and Class Members.

#### **IV. Snowflake breached its duty and engaged in unfair trade practices.**

166. Snowflake breached its duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their customers' PCD and personal information by failing to implement adequate data security practices, which caused the Data Breach.

167. Despite industry guidance at the time of the Data Breach, while Snowflake permitted customers to use MFA, it required customers to opt in. It did not require MFA, including for specific users in customer environments. Additionally, Snowflake did not provide customers with the ability to enforce MFA on its users—i.e., require users to use MFA.

168. A prominent cybersecurity firm executive described the practical failings of Snowflake's MFA configuration as follows<sup>118</sup>:

MFA is a critical component in protecting against identity theft, and specifically against attacks related to the successful theft of passwords through phishing, malware (infostealers), or leakage of reused passwords from compromised sites.

While Snowflake offers users the ability to turn on MFA, this is a feature that is not enabled on users by default and ... it cannot

---

<sup>118</sup> Shane Snider, *Snowflake's Lack of MFA Control Leaves Companies Vulnerable, Experts Say*, Information Week (June 5, 2024), <https://www.informationweek.com/cyber-resilience/snowflake-s-lack-of-mfa-control-leaves-companies-vulnerable-experts-say>. (last visited Mar. 21, 2025).

be enforced on users by the admin of the tenant. This means Snowflake leaves it up to every user to decide whether they want to enroll with MFA or not. This naturally leads to many Snowflake users not having MFA turned on.

Most SaaS vendors, once deployed as an enterprise solution, allow administrators to enforce MFA ... they require every user to enroll in MFA when they first login and make it no longer possible for users to work without it.

169. It was feasible at the time of the Data Breach for Snowflake to allow customers to enforce MFA across their user base. Indeed, on July 9, 2024—less than a month after disclosing the Data Breach—Snowflake rolled out a “new option” to “help admins enforce usage of MFA” by “requir[ing] MFA for all users in an account.” In the announcement, Snowflake touted the enforcement of MFA as a “[b]est practice[.]”<sup>119</sup>

170. It was also feasible at the time of the Data Breach for Snowflake to turn on MFA by default, instead of having it turned off. On September 13, 2024—just three months after disclosing the Data Breach—Snowflake rolled out another new policy enforcing MFA by default on accounts created as of October 2024.<sup>120</sup>

---

<sup>119</sup> Brad Jones and Anoosh Saboori, *Snowflake Admins Can Now Enforce Mandatory MFA*, Snowflake (Jul. 9, 2024), <https://www.snowflake.com/en/blog/snowflake-admins-enforce-mandatory-mfa/>. (last visited Mar. 21, 2025).

<sup>120</sup> Anoosh Saboori & Brad Jones, *Snowflake Strengthens Security with Default Multi-Factor Authentication and Stronger Password Policies*, Snowflake (Sept. 13, 2024), <https://www.snowflake.com/en/blog/multi-factor-identification-default/>. (last visited Mar. 21, 2025).

171. In addition, many of the compromised credentials used by the threat actor were old and had been acquired from malware campaigns dating back to 2020. Snowflake could have closed off this vulnerability by requiring customers to regularly update their credentials, notifying customers to rotate their credentials accordingly, or monitoring info stealer marketplaces for compromised credentials and blocking access by those credentials (something Snowflake now does).

172. Snowflake also could have prevented the Data Breach by maintaining intrusion detection and prevention systems that notify customers of unusual network traffic, such as a login made by a suspicious credential that could be identified by its last login date. Such a system would be consistent with the PCI Cloud Computing Guidelines, which provides, “Since customer access to low level network traffic is impossible, it must rely on Providers for IDS/IPS, monitoring and alerting.”<sup>121</sup>

173. Snowflake, through these data security failings, was negligent and breached its duty to the Plaintiff and Class Members to protect their personal information—information which it knew was sensitive—stored on Snowflake’s Data Cloud.

174. Snowflake’s breach of its duty was a substantial factor in causing the Data Breach. Had Snowflake maintained adequate data security practices (such as

---

<sup>121</sup> *PCI SSC Cloud Computing Guidelines, supra n. 64*, at 63.

requiring or allowing customers to require MFA, credential rotation, or intrusion detection), the Data Breach would have been prevented.

175. Snowflake’s data security failings also constitute an unfair trade practice because of its failure to maintain reasonable and appropriate data security.

176. Rather than take responsibility for its actions, Snowflake foisted the blame and responsibility onto its customers, like Ticketmaster, to “query for unusual activity and conduct further analysis to prevent unauthorized user access.”<sup>122</sup>

177. Despite failing to implement many basic cybersecurity measures, which could have prevented the Data Breach, and despite adopting a “shared responsibility” model, Snowflake insisted that it was not responsible. Snowflake’s CEO Sridhar Ramaswamy’s representation to its investors was, “[a]s extensively reported, the issue wasn’t on the Snowflake side. . . . After multiple investigations by internal and external cybersecurity experts, we found no evidence that our platform was breached or compromised.”<sup>123</sup>

178. Snowflake refuses to take responsibility for its failure to implement basic cybersecurity policies and protocols which would have prevented the Data

---

<sup>122</sup> Alert, *Snowflake Recommends Customers Take Steps to Prevent Unauthorized Access*, CISA (June 3, 2024), <https://www.cisa.gov/news-events/alerts/2024/06/03/snowflake-recommends-customers-take-steps-prevent-unauthorized-access>. (last visited Mar. 21, 2025).

<sup>123</sup> Matt Kapko, *After a wave of attacks, Snowflake insists security burden rests with customers*, CybersecurityDive (Aug. 22, 2024), <https://www.cybersecuritydive.com/news/snowflake-security-responsibility-customers/724994/>. (last visited Mar. 21, 2025).

Breach, even though it has implemented several of those policies since the breach occurred.

179. Based on reports about the Data Breach, upon information and belief, hackers were also able to access the Snowflake platform, which may have caused or contributed to the Data Breach.

#### **PART FOUR: PLAINTIFF'S INJURIES**

180. Plaintiff and Class Members suffered injuries as a result of the Data Breach caused by Defendants' negligent conduct.

181. Beginning on December 17, 2024, Visa issued forty (40) Compromised Account Management System ("CAMS") alerts to NOFFCU. The CAMS alerts stated the estimated fraud "Exposure Window" for the Data Breach was between May 18, 2009, to May 18, 2019. The CAMS alerts further indicated that the Data Breach compromised Primary Account Number ("PAN") data, which is a unique payment card number (credit, debit, or prepaid cards, etc.) that identifies the issuer (financial institution) and the cardholder account. The PAN number is crucial for the issuer to identify the specific account within its systems. PANs are used across various card types including credit, debit, and prepaid cards, and are essential for facilitating electronic financial transactions.

182. In total over 6,000 cards were subject to the CAMS alerts which NOFFCU received related to the Data Breach, of which a substantial number were still active.

183. NOFFCU suffered losses, including but not limited to, time and costs associated with notifying customers that their payment card was compromised in the Data Breach along with the time and costs associated with canceling and reissuing affected cards. To make matters worse, NOFFCU reimbursed customers who suffered fraud losses, currently totaling over several thousand dollars, from the Data Breach on their payment cards and NOFFCU has not been compensated for these losses.

### **CLASS ACTION ALLEGATIONS**

184. Plaintiff brings this action on behalf of itself and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), on behalf of the following class (the “Class”):

All credit unions, banks, and other financial institutions in the United States (including its Territories and the District of Columbia) that issued payment cards that were impacted by the Data Breach announced on or about May 2024.

185. Excluded from the Class are Defendants, any entity in which Defendants have a controlling interest, and Defendants’ officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class

are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

186. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

187. This action may properly be maintained as a class action and satisfies the requirements of Fed. R. Civ. P. 23(a): numerosity, commonality, typicality, and adequacy.

188. Numerosity. The members of the Class are so numerous and geographically dispersed that joinder would be impracticable. The number of Class Members exceeds 100.

189. Commonality and Predominance. There are common questions of law and fact that predominate over questions affecting only individual Class Members. These common legal and factual questions include, but are not limited to:

- whether Defendants owed a duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and members of the Class when obtaining, storing, using, and managing personal information and PCD, including taking action to safeguard such data;
- whether Defendants actively mishandled personal information and PCD and implemented and maintained data security measures that it knew or should have known were unreasonable and inadequate to protect personal information and PCD;
- whether Defendants negligently allowed personal information and PCD to be accessed, used, or disclosed by third parties;



- whether Plaintiff and members of the Class justifiably relied on representations made by Ticketmaster as to their data security practices and the integrity and accuracy of PCD Ticketmaster provided;
- whether Plaintiff and members of the Class justifiably relied on representations made by Ticketmaster that they would oversee and protect PCD and given to third parties like Snowflake and ensure that such entities maintained adequate data security practices and the integrity and accuracy of the PCD Ticketmaster provided;
- whether Ticketmaster intended that Plaintiff and members of the Class would rely on Ticketmaster's representations as to their data security practices and the integrity and accuracy of information Ticketmaster provided;
- whether Ticketmaster failed to adequately notify Plaintiff and members of the Class that their data systems were breached;
- whether Plaintiff and members of the Class were injured and suffered damages and ascertainable losses;
- whether Defendants' actions and inactions failed to provide reasonable security proximately caused the injuries suffered by Plaintiff and members of the Class;
- whether Plaintiff and members of the Class are entitled to damages and, if so, the measure of such damages; and
- whether Plaintiff and members of the Class are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

190. Typicality. Plaintiff's claims are typical of the claims of the absent class members and have a common origin and basis. Plaintiff and absent Class Members are all financial institutions injured by the Data Breach. Plaintiff's claims

arise from the same practices and course of conduct giving rise to the claims of the absent Class Members and are based on the same legal theories, namely the Data Breach. If prosecuted individually, the claims of each Class Member would necessarily rely upon the same material facts and legal theories and seek the same relief. Plaintiff's claims arise from the same practices and course of conduct that give rise to the other Class Members' claims and are based on the same legal theories.

191. Adequacy. Plaintiff will fully and adequately assert and protect the interests of the absent Class Members and have retained Class counsel who are experienced and qualified in prosecuting class action cases similar to this one. Neither Plaintiff nor its attorneys have any interests contrary to or conflicting with the interests of absent Class Members.

192. Predominance. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiff's case will also resolve them for the Class's claims.

193. Superiority. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the absent Class Members' claims is economically infeasible and procedurally impracticable. Class Members share the same factual and legal issues and litigating the claims together will prevent varying, inconsistent, or contradictory judgments,

and will prevent delay and expense to all parties and the court system through litigating multiple trials on the same legal and factual issues. Class treatment will also permit Class Members to litigate their claims where it would otherwise be too expensive or inefficient to do so. Plaintiff knows of no difficulties in managing this action that would preclude its maintenance as a class action.

194. All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendants. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their interests. Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

195. Contact information for each Class Member, including mailing addresses, is readily available, facilitating notice of the pendency of this action.

**CAUSES OF ACTION**

**COUNT I**  
**NEGLIGENCE**

**(On behalf of Plaintiff and the Class against all Defendants)**

196. Plaintiff restates and realleges paragraphs 1–195 as if fully set forth herein.

197. Defendants owe a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and members of the Class when obtaining, storing, using, and managing personal information and PCD, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class of any breach in a timely manner so that appropriate action can be taken to minimize or avoid losses. This duty is independent of any contractual obligations.

198. Defendants have a common law duty to prevent the foreseeable risk of harm to others, including the Plaintiff and the Class. It was certainly foreseeable to Defendants that injury would result from a failure to use reasonable measures to protect PCD and to provide timely notice that a breach was detected. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal PCD belonging to millions of Ticketmaster customers; thieves would use PCD to make large numbers of fraudulent transactions; financial institutions would be required to mitigate the fraud by canceling and reissuing the compromised cards

and reimbursing their customers for fraud losses; and that the resulting financial losses would be immense.

199. Ticketmaster assumed the duty to use reasonable security measures as a result of their conduct to accept payment cards as a method of payment and to oversee the conduct of their vendors such as Snowflake who was entrusted with PCD.

200. In addition to their general duty to exercise reasonable care, Defendants also had a duty of care as a result of the special relationship that existed between themselves and the Plaintiff and members of the Class. The special relationship arose because financial institutions entrusted Defendants with PCD. Only Defendants had the ability to ensure that Ticketmaster's Snowflake account and the systems of Snowflake were sufficient to protect against the harm to financial institutions from the Data Breach

201. Defendants' duty to use reasonable data security measures also arose under §5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Payment Card Data by businesses such as Ticketmaster. The FTC publications and data security breach orders described above further form the basis of Defendants' duty. In addition, individual states have enacted statutes based upon the FTC Act that also create a duty on the

part of Defendants. Defendants' lax and deficient data security measures and failure to promptly notify Plaintiff and the Class of the Data Breach constitute unfair practices in violation of the FTC Act.

202. Defendants' duty to use reasonable care in protecting PCD arose not only as a result of the common law and the statutes described above, but also because they were bound by, and had committed to comply with, industry standards, specifically including duties under PCI DSS.

203. Defendants breached their common law, statutory, and other duties and, thus, were negligent by failing to use reasonable measures to protect Plaintiff's and Class Members' PCD from the hackers who perpetrated the data breach and by failing to provide timely notice of the breach. Upon information and belief, the specific negligent acts and omissions committed by Defendants include, but are not limited to, some, or all, of the following:

- a. failure to protect, store and delete PCD after the time period necessary to authorize the transaction;
- b. failure to implement systems to protect against malware;
- c. failure to comply with industry standards for two-factor authentication and security of PCD;
- d. failure to maintain adequate firewalls;
- e. failure to track and monitor access to their network and PCD;

- f. failure to limit access to PCD to those with a valid purpose;
- g. failure to encrypt Payment Card Data;
- h. failure to adequately staff and fund their data security operations;
- i. failure to use due care in hiring, promoting, and supervising those responsible for their data security operations;
- j. failure to recognize red flags signaling that Defendants' systems were inadequate and that, as a result, the potential for a massive data breach was increasingly likely;
- k. failure to recognize that cybercriminals had infiltrated systems containing PCD and were stealing PCD while the Data Breach was taking place; and
- l. failure to disclose the Data Breach in a timely manner.

204. In connection with the conduct described above, Defendants acted wantonly, recklessly, and with complete disregard for the consequences.

205. As a direct and proximate result of Defendants' negligence, Plaintiff and members of the Class have suffered, and continue to suffer, injury, including, but not limited to, canceling and reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud

monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers. Plaintiff and the Class also lost interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

## **COUNT II**

### **NEGLIGENCE *PER SE***

#### **(On behalf of Plaintiff and the Class against all Defendants)**

206. Plaintiff restates and realleges paragraphs 1–195 as if fully set forth herein.

207. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Ticketmaster, of failing to use reasonable measures to protect Payment Card Data. The FTC publications and orders described above also form part of the basis of Defendants’ duty.

208. Defendants violated §5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff’s and the Class’s PCD and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Defendants’ conduct was particularly unreasonable given the nature and amount of PCD obtained and stored in Ticketmaster’s Snowflake



account, and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers, Plaintiff, and the Class.

209. Defendants' violation of §5 of the FTC Act (and similar state statutes) constitutes negligence per se.

210. Plaintiff and members of the Class are within the class of persons that §5 of the FTC Act (and similar state statutes) was intended to protect, as they are engaged in trade and commerce and bear primary responsibility for directly reimbursing consumers for fraud losses. Moreover, many of the Class Members are credit unions, which are organized as cooperatives whose members are consumers.

211. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by the Plaintiff and the Class.

212. As a direct and proximate result of Defendants' negligence per se, Plaintiff and the Class have suffered, and continue to suffer, injury, including, but not limited to, canceling and reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect

themselves and their customers. They also lost interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

### **COUNT III**

#### **UNJUST ENRICHMENT**

##### **(On behalf of Plaintiff and the Class against all Defendants)**

213. Plaintiff restates and realleges paragraphs 1–195 as if fully set forth herein.

214. Plaintiff and Class Members conferred a monetary benefit on Defendants by providing them with their valuable PCD.

215. Defendants knew that Plaintiff and Class Members conferred a benefit upon them and accepted and retained that benefit by accepting and retaining the PCD entrusted to them.

216. Defendants profited from Plaintiff's and Class Members' PCD and use of Plaintiff's and Class Members' PCD for business purposes.

217. Defendants failed to secure Plaintiff's and Class Members' PCD and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PCD provided.

218. Defendants acquired Plaintiff's and the Class's PCD through inequitable record retention as Defendants failed to disclose the inadequate data security practices previously alleged.

219. If Plaintiff and Class Members had known Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PCD, they would not have agreed to the entrustment of their PCD to Defendants.

220. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon Defendants.

221. Plaintiff and Class Members are without an adequate remedy at law.

222. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered injuries, including those identified above.

223. Plaintiff and Class Members are entitled to restitution and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct, as well as return of their sensitive PCD and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

**COUNT IV**

**DECLARATORY AND INJUNCTIVE RELIEF  
(On behalf of Plaintiff and the Class against all Defendants)**

224. Plaintiff restates and realleges paragraphs 1–195 as if fully set forth herein.

225. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

226. An actual controversy has arisen in the wake of the Data Breach regarding their common law and other duties to reasonably safeguard PCD. Plaintiff alleges that Defendants’ data security measures were inadequate and remain inadequate. Plaintiff anticipates that Defendants will deny these allegations. Furthermore, Plaintiff and Class Members continue to suffer injury as additional cards are identified and need to be reissued and additional fraudulent charges are being made on payment cards they issued to Ticketmaster customers.

227. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendants continue to owe a legal duty to secure Ticketmaster’s customers’ personal and financial information—specifically

including PCD used by Ticketmaster customers—and to notify financial institutions of a data breach under the common law, §5 of the FTC Act, PCI DSS standards, their commitments, and various state statutes;

- b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure their customers' personal information and PCD; and
- c. Defendants' ongoing breaches of their legal duty continue to cause Plaintiff and the Class harm.

228. The Court also should issue corresponding injunctive relief requiring Defendants to employ adequate security protocols, consistent with industry standards, to protect PCD. Specifically, this injunction should, among other things, direct Defendants to:

- a. utilize industry standard encryption to require two-factor authentication for Defendants' computer systems and/or accounts;
- b. require that PCD be encrypted at all other times;
- c. require that Defendants only maintain PCD for a limited time where they have an ongoing need to use such data;

- d. require Defendants to delete all historical PCD that they possess;
- e. engage third-party auditors, consistent with industry standards, to test their systems for weakness and upgrade any such weakness found;
- f. audit, test, and train their data security personnel regarding any new or modified procedures and how to respond to a data breach;
- g. regularly test their systems for security vulnerabilities, consistent with industry standards;
- h. comply with all PCI DSS standards pertaining to the security of their customers' personal and confidential information; and
- i. install all upgrades recommended by manufacturers of security software and firewalls used by Defendants.

229. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Ticketmaster and Snowflake. The risk of another such breach is real, immediate, and substantial. If another breach at Ticketmaster and Snowflake occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to

bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for out-of-pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable and reputational damage.

230. The hardship to Plaintiff and the Class, if an injunction is not issued, exceeds the hardship to Defendants, if an injunction is issued. Among other things, if another massive data breach occurs at Ticketmaster and Snowflake, Plaintiff and members of the Class will likely incur millions of dollars in damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable data security measures is relatively minimal and Defendants have a pre-existing legal obligation to employ such measures.

231. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Ticketmaster and Snowflake, thus eliminating the injuries that would result to Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is the proper class representative; and appoint Plaintiff's counsel as Class Counsel;

B. That the Court award Plaintiff and Class Members damages, including but not limited to the costs of reissuing payment cards, reimbursement for fraudulent charges reimbursed to customers, employee time and expenses in investigating the Data Breach, increased fraud monitoring, as well as compensatory, consequential, general, and/or nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

C. That the Court award punitive or exemplary damages, to the extent permitted by law;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

E. That Plaintiff be granted the declaratory and permanent injunctive relief to prohibit and prevent Defendants from continuing to engage in unlawful acts, omissions and practices described herein and to further injuries to Plaintiff and the Class from manifesting as alleged herein;

F. That the Court award to Plaintiff the costs and disbursements of this action, along with reasonable attorneys' fees, costs, and expenses;



G. That the Court award pre-and post-judgment interest at the maximum legal rate; and,

H. Any other relief that the Court deems just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury of all claims so triable.

Dated: April 7, 2025      Respectfully submitted,

/s/ Domenic A. Cossi  
Domenic A. Cossi, Esq.  
**WESTERN JUSTICE ASSOCIATES, PLLC**  
303 West Mendenhall Street, Suite 1  
Bozeman, MT 59715  
Tel: (406) 587-1900  
Fax: (406) 587-1901  
Email: domenic@westernjusticelaw.com

*One of the Co-Lead Counsel of the Financial  
Institution Spoke*

/s/ Jon Mann  
Jonathan S. Mann (*Admitted Pro Hac Vice*)  
**PITTMAN, DUTTON, HELLUMS, BRADLEY  
& MANN, P.C.**  
2001 Place North, Suite 1100  
Birmingham, AL 35203  
Tel: (205) 322-8880  
Fax: (205) 327-2811  
Email: jonm@pittmandutton.com

*Additional Counsel for Plaintiff and the Proposed  
Class*

**CERTIFICATE OF SERVICE**

I hereby certify that a true and correct copy of the foregoing was filed using this Court's CM/ECF service, which will send notification of such filing to all counsel of record this 7th day of April 2025.

/s/ Domenic A. Cossi

*One of the Co-Lead Counsel for the  
Financial Institution Spoke*